#3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Tsutomu MATSUMOTO, et al.**

Serial No.: **Not Yet Assigned**

Filed: **March 19, 2001**

For: **CARD SETTLEMENT METHOD AND SYSTEM USING MOBILE INFORMATION TERMINAL**

CLAIM FOR PRIORITY UNDER 35 U.S.C. 119

Commissioner for Patents
Washington, D.C. 20231

March 19, 2001

Sir:

The benefit of the filing date of the following prior foreign application is hereby requested for the above-identified application, and the priority provided in 35 U.S.C. 119 is hereby claimed:

Japanese Appln. No. 2000-358016, filed November 24, 2000

In support of this claim, the requisite certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the applicants have complied with the requirements of 35 U.S.C. 119 and that the Patent and Trademark Office kindly acknowledge receipt of said certified copy.

In the event that any fees are due in connection with this paper, please charge our Deposit Account No. 01-2340.

Respectfully submitted,
ARMSTRONG, WESTERMAN, HATTORI
McLELAND & NAUGHTON, LLP

William F. Westerman
Reg. No. 29,988

Atty. Docket No.: 010369
Suite 1000, 1725 K Street, N.W.
Washington, D.C. 20006
Tel: (202) 659-2930
Fax: (202) 887-0357
WFW/ll

日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年１１月２４日

出願番号
Application Number: 特願２０００－３５８０１６

出願人
Applicant (s): 富士通株式会社

２００１年　１月２６日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３０００６３

【書類名】　特許願

【整理番号】　0051073

【提出日】　平成12年11月24日

【あて先】　特許庁長官　及川　耕造　殿

【国際特許分類】　G06F 15/30　340

G11C　7/00　315

H04B　1/034

【発明の名称】　携帯情報端末を利用したカード決済方法及びシステム

【請求項の数】　18

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　松本　勉

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　光本　弘樹

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　鎌田　武志

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100077517

【弁理士】

【氏名又は名称】　石田　敬

【電話番号】　03-5470-1900

【選任した代理人】

【識別番号】　100092624

【弁理士】

【氏名又は名称】　鶴田　準一

【選任した代理人】

【識別番号】　100100871

【弁理士】

【氏名又は名称】　土屋　繁

【選任した代理人】

【識別番号】　100082898

【弁理士】

【氏名又は名称】　西山　雅也

【選任した代理人】

【識別番号】　100081330

【弁理士】

【氏名又は名称】　樋口　外治

【手数料の表示】

【予納台帳番号】　036135

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9905449

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　携帯情報端末を利用したカード決済方法及びシステム

【特許請求の範囲】

【請求項１】　店舗における取引の決済に、ＩＣカード読み書き機能と無線通信機能とを備えた携帯情報端末を利用するカード決済方法であって、

店舗を利用中の顧客により前記携帯情報端末が無線によりネットワーク経由で認証サーバに接続される段階と、

前記顧客により自分のＩＣカードが前記携帯情報端末に装着され、このＩＣカードに格納されている情報が読み取られて前記認証サーバに送られる段階と、

前記ＩＣカードに格納されてカードの正当性を証明する認証情報、少なくともカード番号を含む決済情報、及び顧客により入力されて顧客の正当性を証明する暗証情報から、前記認証サーバにより今回の取引の認証が判断される段階と、

今回の取引の認証後に、決済サーバから発行された一時的なパスワードが前記携帯情報端末に送られて表示される段階と、

一時的なパスワードと今回の取引情報が店舗側の決済端末から入力されて前記決済サーバに送られる段階と、

前記パスワードと取引情報が決済条件を満たした取引について、前記決済サーバにより決済が行われる段階と、

を備えることを特徴とする携帯情報端末を利用したカード決済方法。

【請求項２】　店舗における取引の決済に、ＩＣカード読み書き機能と無線通信機能とを備えた携帯情報端末を利用するカード決済方法であって、

店舗を利用中の顧客により前記携帯情報端末が無線によりネットワーク経由で認証サーバに接続される段階と、

前記顧客により自分のＩＣカード及び前記店舗に備えられた店舗用ＩＣカードが前記携帯情報端末に装着され、これらのＩＣカードに格納されている情報が読み取られて前記認証サーバに送られる段階と、

前記顧客のＩＣカードに格納されて顧客の正当性を証明する認証情報と前記店舗用ＩＣカードに格納されて店舗を特定する店舗情報から、前記認証サーバによりこれらのＩＣカードの適否が前記認証サーバにより判断される段階と、

これらのＩＣカードが認証された後に、顧客から入力されて顧客の正当性を証明する暗証情報により、前記顧客の認証が前記認証サーバにより行われる段階と、

顧客が認証された後に、顧客のＩＣカードに格納されている少なくともカード番号を含む決済情報と顧客により入力された今回の取引情報により、決済サーバにより今回の取引の認証が判断される段階と、

今回の取引が決済条件を満たしたと判断された場合に、前記決済サーバにより決済が行われる段階と、

を備えることを特徴とする携帯情報端末を利用したカード決済方法。

【請求項３】　店舗における取引の決済に、ＩＣカード読み書き機能と近距離無線通信機能とを備えた携帯情報端末と、近距離無線通信機能を備えた店舗側の決済端末を利用するカード決済方法であって、

店舗を利用中の顧客により前記携帯情報端末が無線により店舗側の決済端末に接続される段階と、

前記顧客により自分のＩＣカードが前記携帯情報端末に装着され、このＩＣカードに格納されている情報と、前記顧客から入力されて顧客の正当性を証明する暗証情報が前記決済端末に送られる段階と、

ＩＣカードに格納されていたカードの正当性を証明する認証情報と前記暗証情報が、前記決済端末から決済ネットワークを通じて認証サーバに送られる段階と、

前記認証情報と暗証情報に基づき、前記認証サーバにより、前記ＩＣカードの適否と前記顧客の適否が判断される段階と、

前記ＩＣカードと前記顧客が認証された後、前記顧客によりＩＣカードに格納された少なくともカード番号を含む決済情報、及び顧客により入力された取引情報が無線により前記店舗側の決済端末に入力される段階と、

前記決済端末が今回の取引の有効性を判断する段階と、

有効性の確認後、前記決済端末から今回の取引情報が店舗を特定する店舗情報と共に前記決済ネットワーク経由で決済サーバに送られる段階、及び、

前記決済サーバにより決済が行われる段階と、

を備えることを特徴とする携帯情報端末を利用したカード決済方法。

【請求項４】　請求項１から３の何れか１項に記載の携帯情報端末を利用したカード決済方法であって、更に、前記決済サーバにより前記決済が実行された後に、前記店舗側の決済端末から利用明細が発行されることを特徴とするカード決済方法。

【請求項５】　店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

携帯情報端末に設けられ、カードの正当性を証明する認証情報、顧客の正当性を証明する暗証情報、及び、少なくともカード番号を含む決済情報が格納されたＩＣカードに対して情報の読み書きを行うＩＣカードの読み書き機能、

特定サービス用のアプリケーションソフトウエアの格納、前記携帯情報端末の画面の制御、及び、前記携帯情報端末のネットワークと前記決済ネットワークの間のゲートウエイ機能を提供するアプリケーションサーバ、及び、

前記ＩＣカードから前記携帯情報端末のネットワーク、前記アプリケーションサーバ、及び、前記決済ネットワークを通じて入力された決済情報を基に、一時的なパスワードを発行する、前記決済サーバに設けられたパスワード発行機能とを備えることを特徴とする決済システム。

【請求項６】　請求項５に記載の携帯情報端末を利用したカード決済システムであって、店舗において顧客に代金支払いが発生した際に、以下の手順、

顧客により前記ＩＣカードが装着された前記携帯情報端末が、前記アプリケーションサーバを経由して前記認証サーバに接続され、このＩＣカードに格納された認証情報が前記認証サーバに送出される、

前記ＩＣカードに格納された認証情報に基づき、前記認証サーバによりこのＩＣカードの適否が判断される、

前記カードが適切であると認証された後、顧客により前記携帯情報端末の入力装置から暗証情報が入力されて前記認証サーバに送られる、

暗証情報により顧客が確認された後、顧客により前記ＩＣカードに格納された決済情報が入力されて前記決済サーバに送られる、

前記暗証情報、決済情報、並びに受信時間を基にして、前記決済サーバにより発行された一時的なパスワードが前記携帯情報端末に送られ、その表示器に表示される、

表示された一時的なパスワードと今回の売上情報が前記店舗に設置された前記決済端末から入力される、及び、

前記一時的なパスワードと取引情報が前記決済サーバによりチェックされた後、決済条件を満たした取引について、前記決済サーバからの信号により、前記店舗の決済端末から利用明細が発行される、

により決済が行なわれることを特徴とする携帯情報端末を利用したカード決済システム。

【請求項７】　店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

携帯情報端末に設けられ、少なくともカード番号、カードの有効期限、及び顧客名を含む決済情報が格納された個人用ＩＣカード、及び、少なくとも取引加盟店ＩＤを含む店舗情報が格納された店舗用ＩＣカード、に対して情報の読み書きを行うＩＣカードの読み書き機能、及び、

特定サービス用のアプリケーションソフトウエアの格納、前記携帯情報端末の画面の制御、及び、前記携帯情報端末のネットワークと前記決済ネットワークの間のゲートウエイ機能を提供するアプリケーションサーバと、

を備えることを特徴とする決済システム。

【請求項８】　請求項７に記載の携帯情報端末を利用したカード決済システムであって、店舗において顧客に代金支払いが発生した際に、以下の手順、

前記個人用と店舗用のＩＣカードが装着された前記携帯情報端末が、前記アプリケーションサーバを経由して前記認証サーバに接続され、２つのＩＣカードに格納された個々のカードの正当性を証明する認証情報がそれぞれ前記認証サーバに送出される、

前記ＩＣカードに格納された認証情報に基づき、前記認証サーバにより２つのＩＣカードの適否が判断される、

前記２つのＩＣカードが適切であると認証された後、顧客により前記携帯情報端末の入力装置から暗証情報が入力されて前記認証サーバに送られる、

暗証情報により顧客が確認された後、前記個人用ＩＣカードに格納された決済情報、及び店舗用ＩＣカードに格納された店舗情報と共に前記決済サーバに送られる、及び、

前記決済サーバにより前記決済情報、店舗情報、及び取引情報をチェックされた後、決済条件を満たした取引について、前記決済サーバからの信号により、前記店舗の決済端末から利用明細が発行される、

により決済が行なわれることを特徴とする携帯情報端末を利用したカード決済システム。

【請求項９】　請求項５または７に記載の携帯情報端末を利用したカード決済システムにおいて、

前記アプリケーションサーバが前記携帯情報端末のネットワークと前記決済ネットワークの間に位置するサービスセンタに設けられており、このサービスセンタに前記認証サーバが設けられていることを特徴とするカード決済システム。

【請求項１０】　請求項５または７に記載の携帯情報端末を利用したカード決済システムにおいて、

前記認証サーバに相当する認証機能が前記携帯情報端末に設けられており、前記ＩＣカードの適否の認証が前記携帯情報端末において行なわれることを特徴とするカード決済システム。

【請求項１１】　店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

顧客の所有する携帯情報端末に設けられた無線モジュール、

携帯情報端末に設けられて、少なくともカード番号、カードの有効期限、及び顧客名を含む決済情報が格納されたＩＣカードに対して情報を読み書きするＩＣカードの読み書き機能、及び、

前記携帯情報端末の無線モジュールと交信を行なうことができる前記決済端末に設けられた無線モジュールとを備えることを特徴とする決済システム。

【請求項１２】　請求項１１に記載の携帯情報端末を利用したカード決済システムであって、店舗において顧客に代金支払いが発生した際に、以下の手順、

顧客により前記ＩＣカードが装着された前記携帯情報端末が、前記無線モジュールを介して前記店舗の決済端末に接続され、前記ＩＣカードに格納されてカードの正当性を証明する認証情報と顧客の入力した顧客の正当性を証明する暗証情報が前記決済端末に送出される、

前記決済端末から前記ＩＣカードに格納された認証情報と顧客の入力した暗証情報が前記決済ネットワークを介して前記認証サーバに送出される、

前記認証情報と暗証情報に基づき、前記認証サーバによりこのＩＣカードの適否と利用者の適否が判断される、

前記ＩＣカードと利用者が認証された後、前記ＩＣカードに格納された決済情報、及び入力された取引金額情報と商品情報、が前記無線モジュールを介して前記決済端末に送出される、

前記決済端末により商品と金額の有効性が審査される、

有効性の確認後、前記決済端末から前記決済情報、取引金額情報、及び、店舗情報が前記決済ネットワークを経由して前記認証サーバ経由で前記決済サーバに送出される、及び、

受け取った前記決済情報、取引金額情報、及び、店舗情報を基に前記決済サーバにより当該取引の有効性が審査され、その結果と利用明細が前記決済ネットワーク経由で前記決済端末に送付され、前記店舗の決済端末から利用明細が発行される、

により決済が行なわれることを特徴とする携帯情報端末を利用したカード決済システム。

【請求項１３】　請求項１２に記載の携帯情報端末を利用したカード決済システムにおいて、

前記決済ネットワークと前記決済端末の間にアプリケーションサーバが設けられており、前記認証サーバがこのアプリケーションサーバに設置されていることを特徴とするカード決済システム。

【請求項１４】　請求項１１に記載の携帯情報端末を利用したカード決済システムにおいて、

１台の前記決済端末が前記無線モジュールを介して同時に複数台の携帯情報端末と決済処理が実行できるようになっているカード決済システム。

【請求項１５】　請求項４に記載の携帯情報端末を利用したカード決済方法において、

前記決済サーバにより前記店舗の決済端末から利用明細が発行される際に、前記アプリケーションサーバ経由で前記携帯情報端末の表示器にも決済結果が表示されることを特徴とするカード決済システム。

【請求項１６】　請求項５に記載の携帯情報端末を利用したカード決済システムにおいて、

ＩＣカードの読み書き機能が前記携帯情報端末に外付けされているカード決済システム。

【請求項１７】　請求項５に記載の携帯情報端末を利用したカード決済システムにおいて、

ＩＣカードの読み書き機能が前記携帯情報端末に内蔵されているカード決済システム。

【請求項１８】　請求項５に記載の携帯情報端末を利用したカード決済システムにおいて、

前記携帯情報端末が携帯電話であるカード決済システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は携帯情報端末を利用したカード決済方法及びシステムに関し、特に、ＩＣカードに対して読み書きが可能な携帯情報端末を利用して、無線により購入代金や利用代金の決済を行なうことができるカード決済方法及びシステムに関する。

【０００２】

【従来の技術】

従来、顧客が店舗を利用した際に発生した料金（購入代金、飲食代金、サービス利用代金等）をキャッシュレスで決済する方法として、クレジットカードやデビットカードが普及している。クレジットカードは銀行と商店が提携して行なう信用販売制度に使用するカードであり、銀行に預金口座がある人に対して発行され、クレジット会社が関与している。クレジットカードを使用して代金の決済を行なう場合は、店舗に設置された決済端末であるＣＡＴ端末にクレージットカードの磁気ストライプを読み込ませて決済情報をクレジット会社に送るようになっている。

【０００３】

クレジットカードは直接顧客の銀行口座とは結びついていないので、ＣＡＴ端末からクレジットカードの認証センタに利用者のカード利用を認証しても良いかどうかを問い合わせ（磁気情報を送る）、認証センタがその情報から認証の良否を判断する。認証センタはクレジットカードから読み取られた磁気情報の内容を確認し、カード番号が顧客ブラックリストに載っていないか、または、カードの利用額を越えていないか等をチェックして不正を防止する。このチェックによりクレジットカードに問題がなければ、認証センタからＣＡＴ端末に認証が返信される。そうすると、クレジットカード利用日の２０日～５０日後に伝票が上がって顧客の銀行口座から顧客の利用金額が引かれるようになっている。

【０００４】

このように、クレジットカードによる決済では、店舗の利用日の２０日～５０日後に利用代金が顧客の銀行口座から引き落とされる。一方、近年、信用力の低い人にも発行されるカードシステムであり、即時、もしくは２～３日以内に決済されるカードシステムであるデビットカードが普及し始めている。デビットカードはクレジット会社のネットワークを経由して銀行のホストコンピュータに接続されている。デビットカードは顧客の銀行の口座と直結しているので、支払いが発生したその場で顧客の預金口座から代金が引き落とされる。

【０００５】

ところが、このようなクレジットカードやデビットカードは、カード上の磁気ストライプに決済に必要な情報を記録したものが一般的であり、第三者による磁

気データの不正取得によるカードの不正使用や、磁気ストライプ上のデータの改ざんに対しては、対抗する術がなかった。

この問題を解決すべく登場したのが磁気カードに比べてはるかに大容量、かつカードの中の情報を覗き見られることのない、対タンパー性を備えたＩＣカードである。このＩＣカードはプラスチックカードの内部にＩＣを埋め込んだものであり、欧米ではスマートカードと呼ばれるものである。ＩＣカードは基本的にはＣＰＵ，ＲＯＭ，ＥＥＰＲＯＭ等を内蔵しており、メモリからの情報の入出力をＣＰＵで管理するものである。ＩＣカードは利用者本人のみ知りうる暗証番号で保護されており、第三者による不正使用を防ぐようになっている。また、暗証番号の代わりとして、指紋、音声、虹彩などの生体情報を認証手段として用いることにより、一層のセキュリティの向上を図るようにしたＩＣカードもある。

【０００６】

【発明が解決しようとする課題】

しかしながら、前述のようなＩＣカードの普及には、店舗にＩＣカード読み取り機能付きの端末を設置する必要があり、それには多額に費用が発生するため、ＩＣカードリーダの設置コストの価格がＩＣカードの普及の阻害要因となっているという問題点があった。

【０００７】

そこで、本発明は、店舗側のＣＡＴ端末はそのままにしておいて、ＩＣカードを利用して決済を行なうことができる携帯情報端末を利用したカード決済方法及びシステムを提供することを目的としている。

【０００８】

【課題を解決するための手段】

前記目的を達成する本発明の方法は、以下に第１から第３の発明として示される。

第１の発明は、店舗における取引の決済に、ＩＣカード読み書き機能と無線通信機能とを備えた携帯情報端末を利用するカード決済方法であって、

店舗を利用中の顧客により携帯情報端末が無線によりネットワーク経由で認証サーバに接続される段階と、顧客により自分のＩＣカードが携帯情報端末に装着

され、このＩＣカードに格納されている情報が読み取られて認証サーバに送られる段階と、ＩＣカードに格納されてカードの正当性を証明する認証情報、少なくともカード番号を含む決済情報、及び顧客により入力されて顧客の正当性を証明する暗証情報から、認証サーバにより今回の取引の認証が判断される段階と、今回の取引の認証後に、決済サーバから発行された一時的なパスワードが携帯情報端末に送られて表示される段階と、一時的なパスワードと今回の取引情報が店舗側の決済端末から入力されて決済サーバに送られる段階と、パスワードと取引情報が決済条件を満たした取引について、決済サーバにより決済が行われる段階とを備えることを特徴としている。

【０００９】

第２の発明は、店舗における取引の決済に、ＩＣカード読み書き機能と無線通信機能とを備えた携帯情報端末を利用するカード決済方法であって、

店舗を利用中の顧客により携帯情報端末が無線によりネットワーク経由で認証サーバに接続される段階と、顧客により自分のＩＣカード及び店舗に備えられた店舗用ＩＣカードが携帯情報端末に装着され、これらのＩＣカードに格納されている情報が読み取られて認証サーバに送られる段階と、顧客のＩＣカードに格納されて顧客の正当性を証明する認証情報と店舗用ＩＣカードに格納されて店舗を特定する店舗情報から、認証サーバによりこれらのＩＣカードの適否が認証サーバにより判断される段階と、これらのＩＣカードが認証された後に、顧客から入力されて顧客の正当性を証明する暗証情報により、顧客の認証が認証サーバにより行われる段階と、顧客が認証された後に、顧客のＩＣカードに格納されている少なくともカード番号を含む決済情報と顧客により入力された今回の取引情報により、決済サーバにより今回の取引の認証が判断される段階と、今回の取引が決済条件を満たしたと判断された場合に、決済サーバにより決済が行われる段階とを備えることを特徴としている。

【００１０】

第３の発明は、店舗における取引の決済に、ＩＣカード読み書き機能と近距離無線通信機能とを備えた携帯情報端末と、近距離無線通信機能を備えた店舗側の決済端末を利用するカード決済方法であって、

店舗を利用中の顧客により携帯情報端末が無線により店舗側の決済端末に接続される段階と、顧客により自分のＩＣカードが携帯情報端末に装着され、このＩＣカードに格納されている情報と、顧客から入力されて顧客の正当性を証明する暗証情報が決済端末に送られる段階と、ＩＣカードに格納されていたカードの正当性を証明する認証情報と暗証情報が、決済端末から決済ネットワークを通じて認証サーバに送られる段階と、認証情報と暗証情報に基づき、認証サーバにより、ＩＣカードの適否と顧客の適否が判断される段階と、ＩＣカードと顧客が認証された後、顧客によりＩＣカードに格納された少なくともカード番号を含む情報、及び顧客により入力された取引情報が無線により店舗側の決済端末に入力される段階と、決済端末が今回の取引の有効性を判断する段階と、有効性の確認後、決済端末から今回の取引情報が店舗を特定する店舗情報と共に決済ネットワーク経由で決済サーバに送られる段階、及び、決済サーバにより決済が行われる段階とを備えることを特徴としている。

【００１１】

以上の方法発明において、決済サーバにより決済が実行された後に、店舗側のクレジット照会用端末から利用明細が発行されるようにすることができる。

また、前記目的を達成する本発明のシステムは、以下に第４から第６の発明として示される。

第４の発明は、店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

携帯情報端末に設けられ、カードの正当性を証明する認証情報、顧客の正当性を証明する暗証情報、及び、少なくともカード番号を含む決済情報が格納されたＩＣカードに対して情報の読み書きを行うＩＣカードの読み書き機能、特定サービス用のアプリケーションソフトウエアの格納、携帯情報端末の画面の制御、及び、携帯情報端末のネットワークと決済ネットワークの間のゲートウエイ機能を提供するアプリケーションサーバ、及びＩＣカードから携帯情報端末のネットワーク、アプリケーションサーバ、及び、決済ネットワークを通じて入力された決済情報を基に、一時的なパスワードを発行する、決済サーバに設けられたパスワ

ード発行機能とを備えることを特徴としている。

【００１２】

第５の発明は、店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

携帯情報端末に設けられ、少なくともカード番号、カードの有効期限、及び顧客名を含む決済情報が格納された個人用ＩＣカード、及び、少なくとも取引加盟店ＩＤを含む店舗情報が格納された店舗用ＩＣカードに対して情報の読み書きを行うＩＣカードの読み書き機能、及び、特定サービス用のアプリケーションソフトウエアの格納、携帯情報端末の画面の制御、及び、携帯情報端末のネットワークと決済ネットワークの間のゲートウエイ機能を提供するアプリケーションサーバとを備えることを特徴としている。

【００１３】

第６の発明は、店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

顧客の所有する携帯情報端末に設けられた無線モジュール、携帯情報端末に設けられて、少なくともカード番号、カードの有効期限、及び顧客名を含む決済情報が格納されたＩＣカードに対して情報を読み書きするＩＣカードの読み書き機能、及び、携帯情報端末の無線モジュールと交信を行なうことができる決済端末に設けられた無線モジュールとを備えることを特徴としている。

【００１４】

第１と第４の発明では、ＩＣカードによる決済処理を顧客の携帯情報端末で処理させ、処理結果である決済承認結果と一時的なパスワードを店舗のクレジット照会用端末に送付して、店舗のクレジット照会用端末から一時的なパスワードを再入力させることにより、店舗のクレジット照会用端末に何らＩＣカード読み書き機能を付加することなくＩＣカードによる決済を実現できる。この結果、顧客はＩＣカードによる決済の安全性と、手持ちの携帯情報端末で決済が可能となることによる利便性を得ることができる。

【００１５】

第２と第５の発明では、ＩＣカードによる決済処理を顧客の携帯情報端末で処理させ、かつ、店舗情報も併せて顧客の携帯情報端末で決済サーバに送信することにより、店舗側に決済端末が存在しない場合でも、ＩＣカードによる決済を実現できる。この結果、顧客はＩＣカードによる決済の安全性と、手持ちの携帯情報端末で決済が可能となることによる利便性、及び、店舗側に決済端末が存在しない場合でもＩＣカードによる決済の利便性を得ることができる。

【００１６】

第３と第６の発明では、顧客の携帯情報端末から決済に必要な情報を入力するので、情報の漏洩対策として有効である。また、顧客のカード決済情報はＩＣカードを利用するため、ＩＣカードの安全性の恩恵を受けることができ、不正な取引を防止することが可能である。更に、店舗の決済端末は複数の顧客の携帯情報端末を同時接続して並行処理を行なうことができるので、店舗内の決済端末の縮小と顧客の決済待ち時間の短縮を図ることができ、設備縮小と処理効率可を図ることができる。

【００１７】

【発明の実施の形態】

以下添付図面を用いて本発明の実施形態を具体的な実施例に基づいて詳細に説明する。

図１は本発明の第１、第２の実施形態に使用する携帯情報端末の実施例を示すものである。図１(a)では、携帯電話型の携帯情報端末（インターネットに接続可能な携帯電話のようなものであるが、以後単に携帯電話と記す）１にＩＣカード読み書き装置（図１ではＲ／Ｗと記載）２が取り付けられている。また、図１(b)ではＰＤＡ型の携帯情報端末３にＩＣカード読み書き装置２が取り付けられている。これらの実施形態では、既存の携帯電話１やＰＤＡ型の携帯情報端末３にＩＣカード読み書き装置２を接続するだけで、これらにＩＣカード内の情報を読み取らせることができる。

【００１８】

図２は本発明の第１、第２の実施形態に使用する携帯情報端末である携帯電話

１に接触型のＩＣカード４を組み込む実施例を示すものである。接触型のＩＣカード４はクレジットカードと同じサイズで、データを格納したＩＣ８を内蔵しており、物理的な接点を備えている。図１(a) の実施例では、携帯電話１に設けられたＩＣカード挿入口５にＩＣカード４が差し込まれている。図中の８がＩＣカード４に内蔵されたＩＣである。図１(b) の実施例では、携帯電話１にＩＣカード挿入口５が設けられていると共に、携帯電話１に別のＩＣ９が内蔵されたＩＣカード６が設けられている。そして、ＩＣカード挿入口５にはＩＣカード４が差し込まれている。図１(c) の実施例では、携帯電話１にＩＣカード挿入口５は設けられておらず、別のＩＣ９が内蔵されたＩＣカード６が予め内蔵されているのみである。このように携帯電話１に内蔵されるＩＣカード６はシムカードと呼ばれる。

【００１９】

図３は本発明の第１、第２の実施形態に使用する携帯電話１に非接触型のＩＣカード７を組み込む実施例を示すものである。非接触型のＩＣカード７もクレジットカードと同じサイズであり、カード自体にアンテナがあり、ＩＣチップ８が内蔵されている。データを読み取る携帯電話１の側にもアンテナがあり、電磁誘導方式、或いは静電結合方式により電気を起こしてチップを起動するようになっている。図３(a) では携帯電話１に設けられたＩＣカード挿入口５に非接触型のＩＣカード７が差し込まれている。また、図３(b) では、携帯電話１に設けられたＩＣカード挿入口５に非接触型のＩＣカード７が差し込まれていると共に、携帯電話１にＩＣ９を備えた接触型のＩＣカード６が内蔵されている。

【００２０】

このように、本発明の携帯情報端末を利用したカード決済システムでは、携帯情報端末にＩＣカードのデータを読み取らせたり、また、ＩＣカードにデータを書き込ませたりすることによって決済を行うようになっており、ＩＣカードには前述の３種類の形態がある。よって、ここではこのＩＣカードと携帯情報端末を使用した本発明のカード決済システムの３つの実施形態について、複数の実施例を基に詳細に説明する。

（第１の実施形態）

図４は本発明の携帯情報端末を利用したカード決済システムの第１の実施形態における第１の実施例を示すシステム構成図を示している。

【００２１】

図４において３０は店舗に設置されているクレジット照会用端末であるＣＡＴ端末またはデビット端末であり、決済ネットワークＮＳを通じてカード会社或いは銀行（以後カード会社／銀行と記す）４０に接続されている。従来、通常のクレジットカードやデビットカードを用いて店舗で買物等の取引を行った場合は、このＣＡＴ端末またはデビット端末３０により顧客のカードが読み取られ、決済ネットワークＮＳを通じてカード会社／銀行４０の図示しない認証サーバで認証が得られると、決済サーバ４１により取引の決済が行われる。

【００２２】

また、近年、携帯電話または携帯端末１のような携帯情報端末（以後、代表的に携帯電話１のみを例にとって説明する）はパケット通信網のような携帯無線端末ネットワークＮＲを通じて交信を行うようになっており、インターネットにも接続できるようになってきている。

このような既存のシステムにおいて、本発明の第１の実施形態の第１の実施例では、携帯電話１に内蔵または外付けのＩＣカード読み書き装置（以後ＩＣカードＲ／Ｗと記す）２が接続されており、携帯電話１により顧客の情報が格納されたＩＣカード４に対して情報の読み書きを行えるようになっている。ここでは、携帯電話１、内蔵または外付けＩＣカードＲ／Ｗ２、及びＩＣカード４をまとめて利用者端末１０と呼ぶ。

【００２３】

次に、この実施例では、携帯無線端末ネットワークＮＲと決済ネットワークＮＳの間に位置し、特定サービス用のアプリケーションソフトウエアの格納、携帯電話１の画面の制御、及び、携帯電話１のネットワークＮＲと決済ネットワークＮＳの間のゲートウエイ機能を提供するアプリケーションサーバ２１を備えたサービスセンタ２０が新たに設けられている。そして、このサービスセンタ２０内には、携帯無線端末ネットワークＮＲを通じて携帯電話１から送られてくる顧客のＩＣカード４の情報から、ＩＣカード４の認証及びこのＩＣカード４の利用者

である顧客の認証を行う認証サーバ２２が設けられている。認証サーバ２２は、カードの有効期限やブラックリスト掲載の有無等、決済アプリケーションから見たカードの有効性をチェックする機能を備えている。

【００２４】

更に、第１の実施形態では、カード会社／銀行４０の決済サーバ４１の中に、ＩＣカード４から携帯情報端末のネットワークＮＳ、アプリケーションサーバ２１、及び、決済ネットワークＮＳを通じて入力される決済情報を基に、１度しか利用できないパスワードであるワンタイムパスワードを発行するワンタイムパスワード発行機能が備えられている。ワンタイムパスワードで管理するのは、カード番号、カードの暗証番号、ワンタイムパスワードの有効期限、ワンタイムパスワードの利用限度額等である。ワンタイムパスワードの管理方法としては、(a) パスワードそのものが前述の決済情報を暗号化したデータで、パスワードそのものは決済サーバで保存せず、ＣＡＴ端末からパスワードの提示があった都度データを複合化して決済の妥当性をチェックする方法、(b) パスワードそのものは単なる受付番号的なもので、パスワードに付随する決済情報は全てサーバ側で保存しておき、ＣＡＴ端末からパスワードの提示があった時にサーバで保存されている情報を呼び出して決済処理する方法等が考えられる。

【００２５】

以上のように構成された携帯情報端末を利用したカード決済システムの下で、自己のＩＣカード４を読み込みできるＩＣカードＲ／Ｗ２を備えた携帯電話１を備えた顧客が、ＣＡＴ端末またはデビット端末３０を備えた店舗において、商品を購買する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法について、以下に段階を追って説明する。なお、以下に記す段階番号は図４に太線や破線で示すルートに付された番号に一致している。

【００２６】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は携帯電話１でサービスセンタ２０に電話すると、利用者端末１０とサービスセンタ２０の認証サーバ２２が接続され、携帯電話１の表示窓に「ＩＣカードを読み込ませて下さい」と表示される。

(2) この指示により顧客は自分のＩＣカード４を携帯電話１に読み込ませる。図４ではＩＣカード４は携帯電話１と別体になっているが、このときのＩＣカードの形態は図１～図３で説明したように色々ある。ＩＣカード４の情報はサービスセンタ２０の認証サーバ２２に入力される。サービスセンタ２０の認証サーバ２２は顧客のＩＣカード４に格納された認証情報に基づき、ＩＣカード４を認証すると共に、カードの有効期限やブラックリスト掲載の有無をチェックする。

【００２７】

(3) カードの認証後、顧客本人の認証のため、認証サーバ２２から顧客の携帯電話１からのＩＣカード４の暗証番号の入力が要求される。

(4) 顧客は携帯電話１のキーを使用して暗証番号を入力する。この暗証番号により認証サーバ２２は顧客本人を認証する。

なお、この時の認証方法としては、暗証番号以外にも、指紋、声紋、虹彩等の生体の認証情報をこれらの読み取り装置を使用して読み取って照合するようにすれば、一層のセキュリティを図ることができる。

【００２８】

また、暗証番号による利用者の認証の代わりに、利用者のみ知りうる事柄に関する特殊情報を予めＩＣカードに登録しておき、利用者認証時にこの特殊情報を利用者に入力させてＩＣカード内の特殊情報と比較することにより利用者を認証するようにしても、一層のセキュリティを図ることができる。

(5) 顧客の認証後、ＩＣカード４内に格納されたＩＣクレジット（またはＩＣデビット）情報がアプリケーションサーバ２１を経由して、カード会社／銀行４０の決済サーバ４１に送出される。

【００２９】

(6) カード会社／銀行４０の決済サーバ４１は、受け取ったＩＣカード４の暗証番号およびＩＣクレジット（又はＩＣデビット）情報、並びに受け取った時間を基に、生成された時間からある一定時間内（例えば３０分以内）の１度だけの取引にのみ使用可能なワンタイムパスワード（数字または記号）を生成し、アプリケーションサーバ２１を経由して利用者端末１０の携帯電話１に表示する。

【００３０】

(7) 顧客は携帯電話１に表示されたワンタイムパスワードを店舗のＣＡＴ端末またはデビット端末３０から入力する。この入力は店舗の人が行っても、顧客が直接行っても良い。

(8) ＣＡＴ端末またはデビット端末３０は、顧客の取引情報に入力されたワンタイムパスワードを付加した情報を、決済ネットワークＮＳを通じてカード会社／銀行４０の決済サーバ４１に転送する。

【００３１】

(9) 決済サーバ４１は取引情報とパスワードをチェックした後、決済条件を満たした取引に対して店舗のＣＡＴ端末またはデビット端末３０にデータを転送してカード利用明細を発行する。これで顧客の取引が成立する。

この取引の成立から所定期間後に、通常のクレジット取引と同様に、顧客の銀行の口座から成立した取引金額が店舗の口座に振り替えられる。

【００３２】

図５は、本発明の携帯情報端末を利用したカード決済システムの第１の実施形態における第２の実施例を示すシステム構成図である。第２の実施例が第１の実施例と異なる点は、顧客のＩＣカード４の認証を行う認証サーバの設置位置である。即ち、第１の実施例ではサービスセンタ２０内に顧客のＩＣカード４の認証を行う認証サーバ２２が設けられていたが、第２の実施例ではサービスセンタ２０内ではなく、カード会社／銀行４０内に認証サーバ４２が設けられている点が異なる。

【００３３】

従って、第２の実施例では、自己のＩＣカード４を読み込みできるＩＣカードＲ／Ｗ２を備えた携帯電話１を備えた顧客が、ＣＡＴ端末またはデビット端末３０を備えた店舗において、商品を購買する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法は、認証する部分のみが前述の第１の実施例と異なる。よって、第２の実施例では第１の実施例と異なる部分のみ決済方法を説明する。なお、図５に太線や破線で示されるルート番号は第１の実施例と同様に段階番号を示している。

【００３４】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は携帯電話１でサービスセンタ２０に電話すると、利用者端末１０とサービスセンタ２０の認証サーバ２２が接続され、携帯電話１の表示窓に「ＩＣカードを読み込ませて下さい」と表示される。

(2) この指示により顧客は自分のＩＣカード４を携帯電話４に読み込ませる。図５でもＩＣカード４は携帯電話１と別体になっているが、このときのＩＣカードの形態は図１～図３で説明したように色々ある。ＩＣカード４の情報はサービスセンタ２０のアプリケーションサーバ２１を経由してカード会社／銀行４０内の認証サーバ４２に入力される。認証サーバ４２は顧客のＩＣカード４に格納された認証情報に基づき、ＩＣカード４を認証すると共に、カードの有効期限やブラックリスト掲載の有無をチェックする。

【００３５】

(3) カードの認証後、顧客本人の認証のため、認証サーバ４２から顧客の携帯電話１からの暗証番号の入力が要求される。

(4) 顧客は携帯電話１のキーを使用して暗証番号を入力する。この暗証番号により認証サーバ４２は顧客本人を認証する。

(5) ～(9) の段階は第１の実施例と同様である。

【００３６】

図６は本発明の携帯情報端末を利用したカード決済システムの第１の実施形態における第３の実施例を示すシステム構成図である。第３の実施例が第１の実施例と異なる点は、顧客のＩＣカード４の認証を行う認証サーバの設置位置である。即ち、第１の実施例ではサービスセンタ２０内に顧客のＩＣカード４の認証を行う認証サーバ２２が設けられていたが、第３の実施例ではサービスセンタ２０内ではなく、利用者端末１０内に認証機能１１が設けられている点が異なる。

【００３７】

従って、第３の実施例では、自己のＩＣカード４を読み込みできるＩＣカードＲ／Ｗ２を備えた携帯電話１を備えた顧客が、ＣＡＴ端末またはデビット端末３０を備えた店舗において、商品を購買する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法は、認証する部分のみが前述の第１の実施例と異な

る。よって、第３の実施例では第１の実施例と異なる部分のみ決済方法を説明する。なお、図６に太線や破線で示されるルート番号は第１の実施例と同様に段階番号を示している。

【００３８】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は携帯電話１でサービスセンタ２０に電話すると、利用者端末１０とサービスセンタ２０が接続され、携帯電話１の表示窓に「ＩＣカードを読み込ませて下さい」と表示される。

(2) この指示により顧客は自分のＩＣカード４を携帯電話４に読み込ませる。図６でもＩＣカード４は携帯電話１と別体になっているが、このときのＩＣカードの形態は図１～図３で説明したように色々ある。ＩＣカード４の情報は携帯電話４内の認証機能１１に入力される。認証機能１１は顧客のＩＣカード４に格納された認証情報に基づき、ＩＣカード４を認証すると共に、カードの有効期限やブラックリスト掲載の有無をチェックする。

【００３９】

(3) カードの認証後、顧客本人の認証のため、認証機能１１から顧客の携帯電話１からの暗証番号の入力が要求される。

(4) 顧客は携帯電話１のキーを使用して暗証番号を入力する。この暗証番号により認証機能１１は顧客本人を認証する。

(5) ～(9) の段階は第１の実施例と同様である。

【００４０】

このように、第１の実施形態では、本来は磁気情報を送るＣＡＴ端末またはデビット端末３０からワンタイムパスワード送ることによって、サービスセンタ２０側でワンタイムパスワードの正当性をチェックしてこの取引がＯＫであると認証することができるので、顧客のＩＣカードを認証したり受け付けたりするしくみが店舗側にない時でも取引が可能である。即ち、本実施形態では、ＩＣカードによる決済処理を利用者端末で処理させ、処理結果であるワンタイムパスワードのみを決済端末であるＣＡＴ端末またはデビット端末３０から入力させることにより、ＣＡＴ端末またはデビット端末３０に何らＩＣカード読み書き機能を付加することなく、ＩＣカードによる決済を実現することができる。この結果、顧客

にとっては、ＩＣカードによる決済の安全性と、手持ちの携帯情報端末で決済が可能になることの利便性の双方を享受することができる。

（第２の実施形態）

図７は本発明の携帯情報端末を利用したカード決済システムの第２の実施形態における第１の実施例を示すシステム構成図である。なお、第１の実施形態で説明した施設や構成部材と同じ施設や構成部材には第１の実施形態と同じ符号を付してある。

【００４１】

第２の実施形態においても、図７に示すように、店舗には決済ネットワークＮＳを通じてカード会社／銀行４０に接続されたＣＡＴ端末またはデビット端末３０が必要である。また、携帯情報端末である携帯電話がパケット通信網のような携帯無線端末ネットワークＮＲを通じて交信を行うようになっており、インターネットにも接続できるようになってきていることも必要である。

【００４２】

更に、このような既存のシステムにおいて、本発明の第２の実施形態では、第１の実施形態において必要であったＩＣカード４、携帯電話１に内蔵または外付けのＩＣカードＲ／Ｗ２に加えて、店舗用のＩＣカード３１が必要である。そして、携帯電話１は顧客のＩＣカード４に対して情報の読み書きを行えるようになっていると共に、店舗用のＩＣカード３１内の認証情報も読み込めるようになっている。なお、第２の実施形態でも携帯電話１、内蔵または外付けＩＣカードＲ／Ｗ２、及びＩＣカード４をまとめて利用者端末１０と呼ぶ。

【００４３】

次に、第２の実施形態の第１の実施例では、携帯無線端末ネットワークＮＲと決済ネットワークＮＳの間に位置し、特定サービス用のアプリケーションソフトウエアの格納、携帯電話１の画面の制御、及び、携帯電話１のネットワークＮＲと決済ネットワークＮＳの間のゲートウエイ機能を提供するアプリケーションサーバ２１を備えたサービスセンタ２０が第１の実施形態の第１の実施例と同様に新たに設けられている。そして、このサービスセンタ２０内には、携帯無線端末ネットワークＮＲを通じて携帯電話１から送られてくる顧客のＩＣカード４と店

舗用ＩＣカード３１の情報から、ＩＣカード４と店舗用ＩＣカード３１の認証、及びこのＩＣカード４の利用者である顧客の認証、及び、店舗用ＩＣカード３１の利用者である店舗の店員の認証を行う認証サーバ２２が設けられている。認証サーバ２２は、カードの有効期限やブラックリスト掲載の有無等、決済アプリケーションから見たカードの有効性をチェックする機能を備えている。

【００４４】

一方、第２の実施形態では、カード会社／銀行４０の決済サーバ４１の中にはワンタイムパスワードを発行するワンタイムパスワード発行機能は備えられていない。

以上のように構成された携帯情報端末を利用したカード決済システムの下で、自己のＩＣカード４と店舗用ＩＣカード３１を読み込みできるＩＣカードＲ／Ｗ２を備えた携帯電話１を備えた顧客が、ＣＡＴ端末またはデビット端末３０を備えた店舗において、商品を購買する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法について、以下に段階を追って説明する。なお、以下に記す段階番号は図７に太線で示すルートに付された番号に一致している。

【００４５】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は携帯電話１でサービスセンタ２０に電話すると、利用者端末１０とサービスセンタ２０の認証サーバ２２が接続され、携帯電話１の表示窓に「あなたのＩＣカードと店舗のＩＣカードを読み込ませて下さい」と表示される。

(2) この指示により顧客は自分のＩＣカード４と店舗から借用した店舗用ＩＣカードを携帯電話４に読み込ませる。図７でもＩＣカード４は携帯電話１と別体になっているが、このときのＩＣカードの形態は図１～図３で説明したように色々ある。顧客のＩＣカード４と店舗用ＩＣカード３１の情報はサービスセンタ２０の認証サーバ２２に入力される。サービスセンタ２０の認証サーバ２２は顧客のＩＣカード４と店舗用ＩＣカード３１に格納された認証情報に基づき、ＩＣカード４と店舗用ＩＣカード３１を認証すると共に、カードの有効期限やブラックリスト掲載の有無をチェックする。

【００４６】

(3) カードの認証後、顧客本人及び店舗の店員の認証のため、認証サーバ２２から顧客の携帯電話１からのＩＣカード４の暗証番号及び店舗用ＩＣカード３１の暗証番号の入力が要求される。

(4) 顧客及び店舗の店員は携帯電話１のキーを使用して暗証番号を入力する。この暗証番号により認証サーバ２２は顧客本人及び店舗の店員を認証する。

【００４７】

なお、この時の認証方法としては、暗証番号以外にも、指紋、声紋、虹彩等の生体の認証情報をこれらの読み取り装置を使用して読み取って照合するようにすれば、一層のセキュリティを図ることができる。

(5) 顧客及び店舗の店員の認証後、ＩＣカード４内に格納されたＩＣクレジット（またはＩＣデビット）情報、店舗用ＩＣカード内に格納された店舗情報に加え、店舗での取引金額がアプリケーションサーバ２１を経由して、カード会社／銀行４０の決済サーバ４１に送出される。

【００４８】

(6) カード会社／銀行４０の決済サーバ４１は、受け取ったＩＣカード４の暗証番号、ＩＣクレジット（又はＩＣデビット）情報、並びに店舗用ＩＣカード３１の店舗情報、及び、取引金額情報をもとにして、当該取引の有効性を審査し、その結果をアプリケーションサーバ２１を経由して利用者端末１０の携帯電話１に表示する。

【００４９】

(7) 決済サーバ４１は同時に、決済条件を満たした取引に対して店舗のＣＡＴ端末またはデビット端末３０にデータを転送してカード利用明細を発行する。これで顧客の取引が成立する。ＣＡＴ端末またはデビット端末３０からの利用明細の発行は、店舗側にも取引の控えがないと困るので行うものであるが、必要がない場合には省略することができる。

【００５０】

この取引の成立から所定期間後に、通常のクレジット取引と同様に、顧客の銀行の口座から成立した取引金額が店舗の口座に振り替えられる。

図８は本発明の携帯情報端末を利用したカード決済システムの第２の実施形態

における第２の実施例を示すシステム構成図である。

第２の実施例が第１の実施例と異なる点は、顧客のＩＣカード４及び店舗用ＩＣカード３１の認証を行う認証サーバの設置位置である。即ち、第１の実施例ではサービスセンタ２０内に顧客のＩＣカード４及び店舗用ＩＣカード３１の認証を行う認証サーバ２２が設けられていたが、第２の実施例ではサービスセンタ２０内ではなく、カード会社／銀行４０内に認証サーバ４２が設けられている点が異なる。

【００５１】

従って、第２の実施例では、自己のＩＣカード４と店舗用ＩＣカード３１を読み込みできるＩＣカードＲ／Ｗ２を備えた携帯電話１を備えた顧客が、ＣＡＴ端末またはデビット端末３０を備えた店舗において、商品を購買する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法は、認証する部分のみが前述の第１の実施例と異なる。よって、第２の実施例では第１の実施例と異なる部分のみ決済方法を説明する。なお、図８に太線で示されるルート番号は第１の実施例と同様に段階番号を示している。

【００５２】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は携帯電話１でサービスセンタ２０に電話すると、利用者端末１０とサービスセンタ２０の認証サーバ２２が接続され、携帯電話１の表示窓に「あなたのＩＣカードと店舗のＩＣカードを読み込ませて下さい」と表示される。

(2) この指示により顧客は自分のＩＣカード４と店舗から借用した店舗用ＩＣカード３１を携帯電話４に読み込ませる。図８でもＩＣカード４は携帯電話１と別体になっているが、このときのＩＣカードの形態は図１～図３で説明したように色々ある。ＩＣカード４と店舗用ＩＣカード３１の情報はサービスセンタ２０のアプリケーションサーバ２１を経由してカード会社／銀行４０内の認証サーバ４２に入力される。認証サーバ４２は顧客のＩＣカード４と店舗用ＩＣカード３１に格納された認証情報に基づき、ＩＣカード４を認証すると共に、カードの有効期限やブラックリスト掲載の有無をチェックする。

【００５３】

(3) カードの認証後、顧客本人及び店舗の店員の認証のため、認証サーバ４２から顧客の携帯電話１からの暗証番号の入力が要求される。

(4) 顧客及び店舗の店員は携帯電話１のキーを使用して暗証番号を入力する。この暗証番号により認証サーバ４２は顧客本人及び店舗の店員を認証する。

(5) ～(7) の段階は第１の実施例と同様である。

【００５４】

図９は本発明の携帯情報端末を利用したカード決済システムの第２の実施形態における第３の実施例を示すシステム構成図である。第３の実施例が第１の実施例と異なる点は、顧客のＩＣカード４及び店舗用ＩＣカード３１の認証を行う認証サーバの設置位置である。即ち、第１の実施例ではサービスセンタ２０内に顧客のＩＣカード４及び店舗用ＩＣカード３１の認証を行う認証サーバ２２が設けられていたが、第３の実施例ではサービスセンタ２０内ではなく、利用者端末１０内に認証機能１１が設けられている点が異なる。

【００５５】

従って、第３の実施例では、自己のＩＣカード４と店舗用ＩＣカード３１を読み込みできるＩＣカードＲ／Ｗ２を備えた携帯電話１を備えた顧客が、ＣＡＴ端末またはデビット端末３０を備えた店舗において、商品を購買する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法は、認証する部分のみが前述の第１の実施例と異なる。よって、第３の実施例では第１の実施例と異なる部分のみ決済方法を説明する。なお、図９に太線で示されるルート番号は第１の実施例と同様に段階番号を示している。

【００５６】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は携帯電話１でサービスセンタ２０に電話すると、利用者端末１０とサービスセンタ２０が接続され、携帯電話１の表示窓に「あなたのＩＣカードと店舗用のＩＣカードを読み込ませて下さい」と表示される。

(2) この指示により顧客は自分のＩＣカード４と店舗用のＩＣカード３１を携帯電話４に読み込ませる。図９でもＩＣカード４は携帯電話１と別体になっているが、このときのＩＣカードの形態は図１～図３で説明したように色々ある。Ｉ

Ｃカード４と店舗用のＩＣカード３１の情報は携帯電話４内の認証機能１１に入力される。認証機能１１は顧客のＩＣカード４に格納された認証情報に基づき、ＩＣカード４と店舗用のＩＣカード３１を認証すると共に、カードの有効期限やブラックリスト掲載の有無をチェックする。

【００５７】

(3) カードの認証後、顧客本人及び店舗の店員の認証のため、認証機能１１から顧客の携帯電話１からの暗証番号の入力が要求される。

(4) 顧客及び店舗の店員は携帯電話１のキーを使用して暗証番号を入力する。この暗証番号により認証機能１１は顧客本人及び店舗の店員を認証する。

(5) ～(7) の段階は第１の実施例と同様である。

【００５８】

このように、第２の実施形態では、ＩＣカードによる決済処理を利用者端末で処理させ、かつ店舗情報も合わせて利用者端末より決済サーバに送信することにより、ＣＡＴ端末またはデビット端末３０に何らＩＣカード読み書き機能を付加することなく、ＩＣカードによる決済を実現することができる。また、店舗側にＣＡＴ端末またはデビット端末３０が存在しない場合でもＩＣカードによる決済を実現することができる。この結果、顧客にとっては、ＩＣカードによる決済の安全性と、手持ちの携帯情報端末で決済が可能になることの利便性の双方を享受することができる。

（第３の実施形態）

図１０は本発明の第３の実施形態に使用するＩＣカード４と近距離無線通信モジュール（以後単に無線モジュールという）５０とが装着可能な携帯情報端末である携帯電話１の構成を示すものである。無線モジュール５０には近距離無線通信の業界標準規格「ブルートゥース」に準拠したものを使用することができる。

このブルートゥースは２．４ＧＨｚ帯の電波を使用し、データを含んだ信号を７９の周波数に分けて送り、受けて側が再合成する通信方式である。使用する周波数を１秒間に１６００回変更するために、他の電波やノイズの影響を抑えることができるという長所があり、実用化が進んでいる。また、ブルートゥースは専用の通信チップと超小型アンテナを組み込めば、機器同士が短い信号を出して相

互に確認し、最大７台まで無線で機器を接続することができる。

【００５９】

図１１は図１０に示す携帯電話１と無線モジュール５０の内部構成の実施例を示すものであり、無線モジュール５０は携帯電話１に外付けするタイプである。無線モジュール５０の内部には近距離用ＲＦ部５１とこれに接続する通信インタフェース５２、及び図示しない超小型アンテナが組み込まれている。

携帯電話１の本体内にはＣＰＵ１２があり、このＣＰＵ１２には、ＩＣカードＲ／Ｗ２、遠距離用ＲＦ部１３、入力装置であるキーデバイス１４、ＲＡＭやＲＯＭ等のメモリ１５、通信インタフェース１６等が接続されている。ＩＣカード４はＩＣカードＲ／Ｗ２に挿入されて格納されているデータが読み取られる。また、無線モジュール５０はその通信インタフェース５２が携帯電話１の通信インタフェース１６に接続される。

【００６０】

図１２は図１０に示す携帯電話１と無線モジュール５０の内部構成の別の実施例を示すものであり、無線モジュール５０は携帯電話１に内蔵されるタイプである。無線モジュール５０の内部には近距離用ＲＦ部５１と図示しない超小型アンテナがあり、近距離用ＲＦ部５１は携帯電話１のＣＰＵ１２に直接接続されている。携帯電話１側のその他の構成は図１１と同じであるので、同じ構成部材には同じ符号を付してその説明を省略する。

【００６１】

図１３は本発明の携帯情報端末を利用したカード決済システムの第３の実施形態における第１の実施例を示すシステム構成図である。

第３の実施形態においては、図１３に示すように、店舗に設置された従来のＣＡＴ端末またはデビット端末３０に、携帯電話１に取り付け或いは組み込まれる無線モジュール５０と通信が可能な無線モジュール７０が取り付けられることが必要である。ＣＡＴ端末またはデビット端末３０に無線モジュール７０を加えたものを、ここでは決済端末６０と呼ぶ。決済端末６０は決済ネットワークＮＳを通じてカード会社／銀行４０の決済サーバ４１に接続されている。

【００６２】

このような既存のシステムにおいて、本発明の第３の実施形態では、第１の実施形態において必要であったＩＣカード４、携帯電話１に内蔵または外付けのＩＣカードＲ／Ｗ２に加えて、無線モジュール５０が必要である。そして、携帯電話１は顧客のＩＣカード４に対して情報の読み書きを行えるようになっている。なお、第３の実施形態でも携帯電話１、内蔵または外付けＩＣカードＲ／Ｗ２、ＩＣカード４、及び無線モジュール５０をまとめて利用者端末１０と呼ぶ。

【００６３】

更に、第３の実施形態の第１の実施例では、決済端末６０と決済ネットワークＮＳの間に位置し、特定サービス用のアプリケーションソフトウエアの格納等を行うアプリケーションサーバ２１を備えたサービスセンタ２０が新たに設けられている。そして、このサービスセンタ２０内には、決済端末６０から送られてくる顧客のＩＣカード４の情報から、ＩＣカード４の認証及びこのＩＣカード４の利用者である顧客の認証を行う認証サーバ２２が設けられている。認証サーバ２２は、カードの有効期限やブラックリスト掲載の有無等、決済アプリケーションから見たカードの有効性をチェックする機能を備えている。

【００６４】

以上のように構成された携帯情報端末を利用したカード決済システムの下で、自己のＩＣカード４を読み込みできるＩＣカードＲ／Ｗ２を備え、無線モジュール５０が取り付け或いは内蔵された携帯電話１を備えた顧客が、この無線モジュール５０と交信可能な無線モジュール７０を備えた決済端末６０を備えた店舗において、商品を購買する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法について、以下に段階を追って説明する。なお、以下に記す段階番号は図１３に太線で示すルートに付された番号に一致している。

【００６５】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は自分のＩＣカード４を携帯電話１に読み込ませた上で、利用者端末１０の無線モジュール５０と店舗の決済端末６０の無線モジュール７０との間で通信を行う。店舗の決済端末６０はサービスセンタ２０の認証サーバ２２に接続されているので、顧客のＩＣカード４内の認証情報は、店舗の決済端末６０を経由してサービスセンタ２０の認

証サーバ２２に入力される。すなわち、ＩＣカード４の正当性を確認するための認証情報が利用者端末１０から店舗の決済端末６０を中継してサービスセンタ２０の認証サーバ２２に送信される。

【００６６】

認証サーバ２２は顧客が本人であるか否かを確認するために、決済端末６０を介して利用者端末１０に暗証番号の入力を要求し、顧客はこの要求に応じて暗証番号を利用者端末１０より入力する。この暗証番号は決済端末６０を介して認証サーバ２２に送信される。

(2) 認証サーバ２２は利用者端末１０のＩＣカード４内に格納された認証情報と、顧客が利用者端末から入力した暗証番号に基づき、利用者端末と利用者を認証し、ＩＣカード４の認証結果を店舗側決済端末６０、無線モジュール７０，５０を介して利用者端末１０に送信する。

【００６７】

(3) 認証後、利用者端末１０のＩＣカード４内に格納されたＩＣクレジット情報（またはＩＣデビット情報）及び店舗での取引金額と商品情報を、顧客が利用者端末１０の入力装置より入力し、ＩＣカード内のデータは無線モジュール５０，７０により店舗のＣＡＴ端末またはデビット端末３０に送信され、ＣＡＴ端末またはデビット端末３０で商品とその取引金額の有効性を審査する。

【００６８】

(4) 有効性が確認された後、店舗の決済端末６０はＩＣクレジット情報（またはＩＣデビット情報）、店舗での取引金額と商品情報、及び決済端末６０に格納された店舗情報（店舗ＩＤ）をサービスセンタ２０のアプリケーションサーバ２１に送出する。

(5) アプリケーションサーバ２１は利用者端末１０から受け取ったＩＣクレジット情報（またはＩＣデビット情報）、店舗での取引金額と商品情報、及び店舗情報を、決済ネットワークＮＳを経由してカード会社／銀行４０の決済サーバ４１に転送する。

【００６９】

(6) カード会社／銀行４０の決済サーバ４１は、認証サーバ２２から受け取っ

たＩＣクレジット情報（またはＩＣデビット情報）、店舗情報及び店舗での取引金額情報を基に、当該取引の有効性を審査し、決済条件を満たした取引に対して店舗の決済端末６０にデータを転送してカード利用明細を発行する。これで顧客の取引が成立する。カード利用明細は決済端末６０から無線モジュール７０，５０を介して利用者端末１０にも送られる。

【００７０】

この取引の成立から所定期間後に、通常のクレジット取引と同様に、顧客の銀行の口座から成立した取引金額が店舗の口座に振り替えられる。

図１４は本発明の携帯情報端末を利用したカード決済システムの第３の実施形態における第２の実施例を示すシステム構成図である。

第３の実施形態の第２の実施例では、図１４に示すように、ＩＣカード４に読み書きを行うために携帯電話１に内蔵または外付けされたＩＣカードＲ／Ｗ２に加えて、無線モジュール５０が必要であると共に、店舗に設置された従来のＣＡＴ端末またはデビット端末３０に、携帯電話１に取り付け或いは組み込まれる無線モジュール５０と通信が可能な無線モジュール７０が取り付けられることが必要である。

【００７１】

第２の実施例でも携帯電話１、内蔵または外付けのＩＣカードＲ／Ｗ２、ＩＣカード４、及び無線モジュール５０をまとめて利用者端末１０と呼ぶと共に、ＣＡＴ端末またはデビット端末３０に無線モジュール７０を加えたものを決済端末６０と呼ぶ。決済端末６０は決済ネットワークＮＳを通じてカード会社／銀行４０の決済サーバ４１に接続されている。第２の実施例では決済端末６０と決済ネットワークＮＳの間にサービスセンタ２０は設けられていない。従って、第２の実施例では、決済サーバ４１と認証サーバ４２は共にカード会社／銀行４０の中に設けられている。

【００７２】

以上のように構成された携帯情報端末を利用したカード決済システムの下で、自己のＩＣカード４を読み込みできるＩＣカードＲ／Ｗ２を備え、無線モジュール５０が取り付け或いは内蔵された携帯電話１を備えた顧客が、この無線モジュ

ール５０と交信可能な無線モジュール７０を備えた決済端末６０を備えた店舗において、商品を購買する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法について、図１４と図１５を用いて段階を追って説明する。なお、図１５に記す段階番号は、図１４に太線で示すルートに付された番号に一致している。

【００７３】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は自分のＩＣカード４を携帯電話１に読み込ませた上で、利用者端末１０の無線モジュール５０と店舗の決済端末６０の無線モジュール７０との間で通信を行う。店舗の決済端末６０は決済ネットワークＮＳを通じてカード会社／銀行４０の認証サーバ４２に接続されているので、顧客のＩＣカード４内の認証情報は、店舗の決済端末６０を経由して認証サーバ４２に入力される。すなわち、ＩＣカード４の正当性を確認するための認証情報が利用者端末１０から店舗の決済端末６０を中継して認証サーバ４２に送信される。

【００７４】

認証サーバ４２は顧客が本人であるか否かを確認するために、決済端末６０を介して利用者端末１０に暗証番号の入力を要求し、顧客はこの要求に応じて暗証番号を利用者端末１０に入力する。この暗証番号は決済端末６０を介して認証サーバ４２に送信される。

(2) 認証サーバ４２は利用者端末１０のＩＣカード４内に格納された認証情報と、顧客が利用者端末から入力した暗証番号に基づき、利用者端末と利用者を認証し、ＩＣカード４の認証結果を店舗側決済端末６０、無線モジュール７０，５０を介して利用者端末１０に送信する。

【００７５】

(3) 認証後、利用者端末１０のＩＣカード４内に格納されたＩＣクレジット情報（またはＩＣデビット情報）及び店舗での取引金額と商品情報を、顧客が利用者端末１０の入力装置より入力し、ＩＣカード内のデータは無線モジュール５０，７０により店舗の決済端末６０に送信され、決済端末６０で商品とその取引金額の有効性を審査する。

【００７６】

(4) 有効性が確認された後、店舗の決済端末６０はＩＣクレジット情報（またはＩＣデビット情報）、店舗での取引金額と商品情報、及び決済端末６０に格納された店舗情報（店舗ＩＤ）をカード会社／銀行４０の決済サーバ４１に送出する。

(5) カード会社／銀行４０の決済サーバ４１は、決済端末６０から受け取ったＩＣクレジット情報（またはＩＣデビット情報）、店舗情報及び店舗での取引金額情報を基に、当該取引の有効性を審査し、決済条件を満たした取引に対して店舗の決済端末６０にＩＣカードデータの認証及び決済された結果と利用明細を送出する。

【００７７】

(6) 決済端末６０は決済結果と利用明細を利用者端末１０に送出し、これで顧客の取引が成立する。

この取引の成立から所定期間後に、通常のクレジット取引と同様に、顧客の銀行の口座から成立した取引金額が店舗の口座に振り替えられる。

図１６は本発明の携帯情報端末を利用したカード決済システムの第３の実施形態の適用例を示すものである。前述のように、無線モジュール５０にブルートゥースを使用した場合、機器同士が短い信号を出して相互に確認し、最大７台まで無線で機器を接続することができる。よって、１つの店舗において、１台の決済端末６０をマスターとした場合、スレーブとして無線モジュール５０Ａ～５０Ｇを備えた最大７台の利用者端末１０Ａ～１０Ｇと取引を行うことができる。この場合、各利用者端末１０Ａ～１０Ｇを識別するために、無線モジュール間の交信には識別コードＡ～Ｇが追加される。

【００７８】

このように第３の実施形態でも利用者端末から決済に必要な情報を入力するため、情報の漏洩に対して有効であり、利用者のカード決済情報はＩＣカードを利用するため、ＩＣカードの安全性の恩恵を受けることができ、不正な取引を防止することが可能である。また、第３の実施形態では、複数の利用者端末からの同時接続を可能とし、並行して処理を行うことができるので、店舗内の決済端末の

装置数の削減と顧客の決済待ち時間の短縮が実現でき、設備削減と処理の効率化を図ることができる。

【００７９】

なお、以上の実施例では、携帯情報端末として携帯電話の実施例を説明したが、携帯電話の代わりにインターネットのようなネットワーク網と接続が可能な携帯型のコンピュータを用いても同様の決済を行うことができる。

（付記１）　店舗における取引の決済に、ＩＣカード読み書き機能と無線通信機能とを備えた携帯情報端末を利用するカード決済方法であって、

店舗を利用中の顧客により前記携帯情報端末が無線によりネットワーク経由で認証サーバに接続される段階と、

前記顧客により自分のＩＣカードが前記携帯情報端末に装着され、このＩＣカードに格納されている情報が読み取られて前記認証サーバに送られる段階と、

前記ＩＣカードに格納されてカードの正当性を証明する認証情報、少なくともカード番号を含む決済情報、及び顧客により入力されて顧客の正当性を証明する暗証情報から、前記認証サーバにより今回の取引の認証が判断される段階と、

今回の取引の認証後に、決済サーバから発行された一時的なパスワードが前記携帯情報端末に送られて表示される段階と、

一時的なパスワードと今回の取引情報が店舗側の決済端末から入力されて前記決済サーバに送られる段階と、

前記パスワードと取引情報が決済条件を満たした取引について、前記決済サーバにより決済が行われる段階と、

を備えることを特徴とする携帯情報端末を利用したカード決済方法。

【００８０】

（付記２）　店舗における取引の決済に、ＩＣカード読み書き機能と無線通信機能とを備えた携帯情報端末を利用するカード決済方法であって、

店舗を利用中の顧客により前記携帯情報端末が無線によりネットワーク経由で認証サーバに接続される段階と、

前記顧客により自分のＩＣカード及び前記店舗に備えられた店舗用ＩＣカードが前記携帯情報端末に装着され、これらのＩＣカードに格納されている情報が読

み取られて前記認証サーバに送られる段階と、

前記顧客のＩＣカードに格納されて顧客の正当性を証明する認証情報と前記店舗用ＩＣカードに格納されて店舗を特定する店舗情報から、前記認証サーバによりこれらのＩＣカードの適否が前記認証サーバにより判断される段階と、

これらのＩＣカードが認証された後に、顧客から入力されて顧客の正当性を証明する暗証情報により、前記顧客の認証が前記認証サーバにより行われる段階と、

顧客が認証された後に、顧客のＩＣカードに格納されている少なくともカード番号を含む決済情報と顧客により入力された今回の取引情報により、決済サーバにより今回の取引の認証が判断される段階と、

今回の取引が決済条件を満たしたと判断された場合に、前記決済サーバにより決済が行われる段階と、

を備えることを特徴とする携帯情報端末を利用したカード決済方法。

【００８１】

（付記３）　店舗における取引の決済に、ＩＣカード読み書き機能と近距離無線通信機能とを備えた携帯情報端末と、近距離無線通信機能を備えた店舗側の決済端末を利用するカード決済方法であって、

店舗を利用中の顧客により前記携帯情報端末が無線により店舗側の決済端末に接続される段階と、

前記顧客により自分のＩＣカードが前記携帯情報端末に装着され、このＩＣカードに格納されている情報と、前記顧客から入力されて顧客の正当性を証明する暗証情報が前記決済端末に送られる段階と、

ＩＣカードに格納されていたカードの正当性を証明する認証情報と前記暗証情報が、前記決済端末から決済ネットワークを通じて認証サーバに送られる段階と、

前記認証情報と暗証情報に基づき、前記認証サーバにより、前記ＩＣカードの適否と前記顧客の適否が判断される段階と、

前記ＩＣカードと前記顧客が認証された後、前記顧客によりＩＣカードに格納された少なくともカード番号を含む情報、及び顧客により入力された取引情報が

無線により前記店舗側の決済端末に入力される段階と、

前記決済端末が今回の取引の有効性を判断する段階と、

有効性の確認後、前記決済端末から今回の取引情報が店舗を特定する店舗情報と共に前記決済ネットワーク経由で決済サーバに送られる段階、及び、

前記決済サーバにより決済が行われる段階と、

を備えることを特徴とする携帯情報端末を利用したカード決済方法。

【００８２】

（付記４）　付記１から３の何れか１項に記載の携帯情報端末を利用したカード決済方法であって、更に、前記決済サーバにより前記決済が実行された後に、前記店舗側の決済端末から利用明細が発行されることを特徴とするカード決済方法。

（付記５）　店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

携帯情報端末に設けられ、カードの正当性を証明する認証情報、顧客の正当性を証明する暗証情報、及び、少なくともカード番号を含む決済情報が格納されたＩＣカードに対して情報の読み書きを行うＩＣカードの読み書き機能、

特定サービス用のアプリケーションソフトウエアの格納、前記携帯情報端末の画面の制御、及び、前記携帯情報端末のネットワークと前記決済ネットワークの間のゲートウエイ機能を提供するアプリケーションサーバ、及び、

前記ＩＣカードから前記携帯情報端末のネットワーク、前記アプリケーションサーバ、及び、前記決済ネットワークを通じて入力された決済情報を基に、一時的なパスワードを発行する、前記決済サーバに設けられたパスワード発行機能とを備えることを特徴とする決済システム。

【００８３】

（付記６）　付記５に記載の携帯情報端末を利用したカード決済システムであって、店舗において顧客に代金支払いが発生した際に、以下の手順、

顧客により前記ＩＣカードが装着された前記携帯情報端末が、前記アプリケーションサーバを経由して前記認証サーバに接続され、このＩＣカードに格納され

た認証情報が前記認証サーバに送出される、

前記ＩＣカードに格納された認証情報に基づき、前記認証サーバによりこのＩＣカードの適否が判断される、

前記カードが適切であると認証された後、顧客により前記携帯情報端末の入力装置から暗証情報が入力されて前記認証サーバに送られる、

暗証情報により顧客が確認された後、顧客により前記ＩＣカードに格納された決済情報が入力されて前記決済サーバに送られる、

前記暗証情報、決済情報、並びに受信時間を基にして、前記決済サーバにより発行された一時的なパスワードが前記携帯情報端末に送られ、その表示器に表示される、

表示された一時的なパスワードと今回の売上情報が前記店舗に設置された前記決済端末から入力される、及び、

前記一時的なパスワードと取引情報が前記決済サーバによりチェックされた後、決済条件を満たした取引について、前記決済サーバからの信号により、前記店舗の決済端末から利用明細が発行される、

により決済が行なわれることを特徴とする携帯情報端末を利用したカード決済システム。

【００８４】

（付記７）　店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

携帯情報端末に設けられ、少なくともカード番号、カードの有効期限、及び顧客名を含む決済情報が格納された個人用ＩＣカード、及び、少なくとも取引加盟店ＩＤを含む店舗情報が格納された店舗用ＩＣカードに対して情報の読み書きを行うＩＣカードの読み書き機能、及び、

特定サービス用のアプリケーションソフトウエアの格納、前記携帯情報端末の画面の制御、及び、前記携帯情報端末のネットワークと前記決済ネットワークの間のゲートウエイ機能を提供するアプリケーションサーバと、

を備えることを特徴とする決済システム。

【００８５】

（付記８）　付記７に記載の携帯情報端末を利用したカード決済システムであって、店舗において顧客に代金支払いが発生した際に、以下の手順、

前記個人用と店舗用のＩＣカードが装着された前記携帯情報端末が、前記アプリケーションサーバを経由して前記認証サーバに接続され、２つのＩＣカードに格納された個々のカードの正当性を証明する認証情報がそれぞれ前記認証サーバに送出される、

前記ＩＣカードに格納された認証情報に基づき、前記認証サーバにより２つのＩＣカードの適否が判断される、

前記２つのＩＣカードが適切であると認証された後、顧客により前記携帯情報端末の入力装置から暗証情報が入力されて前記認証サーバに送られる、

暗証情報により顧客が確認された後、前記個人用ＩＣカードに格納された決済情報、及び店舗用ＩＣカードに格納された店舗情報と共に前記決済サーバに送られる、及び、

前記決済サーバにより前記決済情報、店舗情報、及び取引情報をチェックされた後、決済条件を満たした取引について、前記決済サーバからの信号により、前記店舗の決済端末から利用明細が発行される、

により決済が行なわれることを特徴とする携帯情報端末を利用したカード決済システム。

【００８６】

（付記９）　付記５または７に記載の携帯情報端末を利用したカード決済システムにおいて、

前記アプリケーションサーバが前記携帯情報端末のネットワークと前記決済ネットワークの間に位置するサービスセンタに設けられており、このサービスセンタに前記認証サーバが設けられていることを特徴とするカード決済システム。

【００８７】

（付記１０）　付記５または７に記載の携帯情報端末を利用したカード決済システムにおいて、

前記認証サーバに相当する認証機能が前記携帯情報端末に設けられており、前

記ＩＣカードの適否の認証が前記携帯情報端末において行なわれることを特徴とするカード決済システム。

【００８８】

（付記１１）　店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

顧客の所有する携帯情報端末に設けられた無線モジュール、

携帯情報端末に設けられて、少なくともカード番号、カードの有効期限、及び顧客名を含む決済情報が格納されたＩＣカードに対して情報を読み書きするＩＣカードの読み書き機能、及び、

前記携帯情報端末の無線モジュールと交信を行なうことができる前記決済端末に設けられた無線モジュールとを備えることを特徴とする決済システム。

【００８９】

（付記１２）　付記１１に記載の携帯情報端末を利用したカード決済システムであって、店舗において顧客に代金支払いが発生した際に、以下の手順、

顧客により前記ＩＣカードが装着された前記携帯情報端末が、前記無線モジュールを介して前記店舗の決済端末に接続され、前記ＩＣカードに格納されてカードの正当性を証明する認証情報と顧客の入力した顧客の正当性を証明する暗証情報が前記決済端末に送出される、

前記決済端末から前記ＩＣカードに格納された認証情報と顧客の入力した暗証情報が前記決済ネットワークを介して前記認証サーバに送出される、

前記認証情報と暗証情報に基づき、前記認証サーバによりこのＩＣカードの適否と利用者の適否が判断される、

前記ＩＣカードと利用者が認証された後、前記ＩＣカードに格納された決済情報、及び入力された取引金額情報と商品情報、が前記無線モジュールを介して前記決済端末に送出される、

前記決済端末により商品と金額の有効性が審査される、

有効性の確認後、前記決済端末から前記決済情報、取引金額情報、及び、店舗情報が前記決済ネットワークを経由して前記認証サーバ経由で前記決済サーバに

送出される、及び、

受け取った前記決済情報、取引金額情報、及び、店舗情報を基に前記決済サーバにより当該取引の有効性が審査され、その結果と利用明細が前記決済ネットワーク経由で前記決済端末に送付され、前記店舗の決済端末から利用明細が発行される、

により決済が行なわれることを特徴とする携帯情報端末を利用したカード決済システム。

【００９０】

（付記１３）　付記１２に記載の携帯情報端末を利用したカード決済システムにおいて、

前記決済ネットワークと前記決済端末の間にアプリケーションサーバが設けられており、前記認証サーバがこのアプリケーションサーバに設置されていることを特徴とするカード決済システム。

【００９１】

（付記１４）　付記１１に記載の携帯情報端末を利用したカード決済システムにおいて、

１台の前記決済端末が前記無線モジュールを介して同時に複数台の携帯情報端末と決済処理が実行できるようになっているカード決済システム。

（付記１５）　付記４に記載の携帯情報端末を利用したカード決済方法において、

前記決済サーバにより前記店舗の決済端末から利用明細が発行される際に、前記アプリケーションサーバ経由で前記携帯情報端末の表示器にも決済結果が表示されることを特徴とするカード決済システム。

【００９２】

（付記１６）　付記１から１５の何れか１項に記載の携帯情報端末を利用したカード決済システムにおいて、

前記暗証番号による利用者の認証の代わりに、利用者の指紋、声紋、虹彩等の生体情報を生体情報リーダにより予めＩＣカードに登録しておき、利用者認証時にこの生体情報リーダにより生体情報を読み込んでＩＣカード内の生体情報と比

較することにより利用者を認証するカード決済システム。

【００９３】

（付記１７）　付記１から１５の何れか１項に記載の携帯情報端末を利用したカード決済システムにおいて、

前記暗証番号による利用者の認証の代わりに、利用者のみ知りうる事柄に関する特殊情報を予めＩＣカードに登録しておき、利用者認証時にこの特殊情報を利用者に入力させてＩＣカード内の特殊情報と比較することにより利用者を認証するカード決済システム。

【００９４】

（付記１８）　付記５に記載の携帯情報端末を利用したカード決済システムにおいて、

ＩＣカードの読み書き機能が前記携帯情報端末に外付けされているカード決済システム。

（付記１９）　付記５に記載の携帯情報端末を利用したカード決済システムにおいて、

ＩＣカードの読み書き機能が前記携帯情報端末に内蔵されているカード決済システム。

【００９５】

（付記２０）　付記５に記載の携帯情報端末を利用したカード決済システムにおいて、

前記携帯情報端末が携帯電話であるカード決済システム。

【００９６】

【発明の効果】

以上説明したように、本発明の携帯情報端末を利用したカード決済方法及びシステムによれば、以下のような効果がある。

第１と第４の発明では、ＩＣカードによる決済処理を顧客の携帯情報端末で処理させ、処理結果である決済承認結果とワンタイムパスワードを店舗の決済端末に送付して、店舗の決済端末からワンタイムパスワードを再入力させることにより、店舗の決済端末に何らＩＣカード読み書き機能を付加することなくＩＣカー

ドによる決済を実現できる。この結果、顧客はＩＣカードによる決済の安全性と、手持ちの携帯情報端末で決済が可能となることによる利便性を得ることができる。

【００９７】

第２と第５の発明では、ＩＣカードによる決済処理を顧客の携帯情報端末で処理させ、かつ、店舗情報も併せて顧客の携帯情報端末で決済サーバに送信することにより、店舗側に決済端末が存在しない場合でも、ＩＣカードによる決済を実現できる。この結果、顧客はＩＣカードによる決済の安全性と、手持ちの携帯情報端末で決済が可能となることによる利便性、及び、店舗側に決済端末が存在しない場合でもＩＣカードによる決済の利便性を得ることができる。

【００９８】

第３と第６の発明では、顧客の携帯情報端末から決済に必要な情報を入力するので、情報の漏洩対策として有効である。また、顧客のカード決済情報はＩＣカードを利用するため、ＩＣカードの安全性の恩恵を受けることができ、不正な取引を防止することが可能である。更に、店舗の決済端末は複数の顧客の携帯情報端末を同時接続して並行処理を行なうことができるので、店舗内の決済端末の縮小と顧客の決済待ち時間の短縮を図ることができ、設備縮小と処理効率可を図ることができる。

【図面の簡単な説明】

【図１】

本発明の第１、第２の実施形態に使用する携帯情報端末の実施例を示すものであり、(a) は携帯電話型の携帯情報端末にＩＣカード読み書き装置が取り付けられた状態を示す図、(b) はＰＤＡ型の携帯情報端末にＩＣカード読み書き装置が取り付けられた状態を示す図である。

【図２】

本発明の第１、第２の実施形態に使用する携帯情報端末である携帯電話に接触型のＩＣカードを組み込む実施例を示すものであり、(a) は携帯電話に設けられたＩＣカード挿入口にＩＣカードが差し込まれた状態を示す図、(b) は携帯電話に設けられたＩＣカード挿入口にＩＣカードが差し込まれていると共に、携帯電

話に別のＩＣカードが内蔵されている状態を示す図、(c) はＩＣカードが内蔵された携帯電話の例を示す図である。

【図３】

本発明の第１、第２の実施形態に使用する携帯情報端末である携帯電話に非接触型のＩＣカードを組み込む実施例を示すものであり、(a) は携帯電話に設けられたＩＣカード挿入口に非接触型のＩＣカードが差し込まれた状態を示す図、(b) は携帯電話に設けられたＩＣカード挿入口に非接触型のＩＣカードが差し込まれていると共に、携帯電話に接触型のＩＣカードが内蔵されている状態を示す図である。

【図４】

本発明の携帯情報端末を利用したカード決済システムの第１の実施形態における第１の実施例を示すシステム構成図である。

【図５】

本発明の携帯情報端末を利用したカード決済システムの第１の実施形態における第２の実施例を示すシステム構成図である。

【図６】

本発明の携帯情報端末を利用したカード決済システムの第１の実施形態における第３の実施例を示すシステム構成図である。

【図７】

本発明の携帯情報端末を利用したカード決済システムの第２の実施形態における第１の実施例を示すシステム構成図である。

【図８】

本発明の携帯情報端末を利用したカード決済システムの第２の実施形態における第２の実施例を示すシステム構成図である。

【図９】

本発明の携帯情報端末を利用したカード決済システムの第２の実施形態における第３の実施例を示すシステム構成図である。

【図１０】

本発明の第３の実施形態に使用するＩＣカードと近距離無線通信モジュールと

が装着可能な携帯情報端末である携帯電話の構成を示す斜視図である。

【図１１】

図１０に示す携帯電話と近距離無線通信モジュールの内部構成の一例を示すブロック回路図である。

【図１２】

図１０に示す携帯電話と近距離無線通信モジュールの内部構成の別の例を示すブロック回路図である。

【図１３】

本発明の携帯情報端末を利用したカード決済システムの第３の実施形態における第１の実施例を示すシステム構成図である。

【図１４】

本発明の携帯情報端末を利用したカード決済システムの第３の実施形態における第２の実施例を示すシステム構成図である。

【図１５】

図１４に示すシステムの無線モジュール間の決済シーケンスを示すシーケンス図である。

【図１６】

本発明の携帯情報端末を利用したカード決済システムの第３の実施形態の適用例を示すシステム構成図である。

【符号の説明】

１…携帯電話型の携帯情報端末（携帯電話）

２…ＩＣカード読み書き装置

３…ＰＤＡ型の携帯情報端末

４…接触型のＩＣカード

５…ＩＣカード挿入孔

６…ＩＣカード

７…非接触型ＩＣカード

８，９…ＩＣ

１０…利用者端末

１１…認証機能

２０…サービスセンタ

２１…アプリケーションサーバ

３０…ＣＡＴ／デビット端末

３１…店舗用ＩＣカード

４０…カード会社／銀行

４１…決済サーバ

４２…認証サーバ

５０…無線通信モジュール

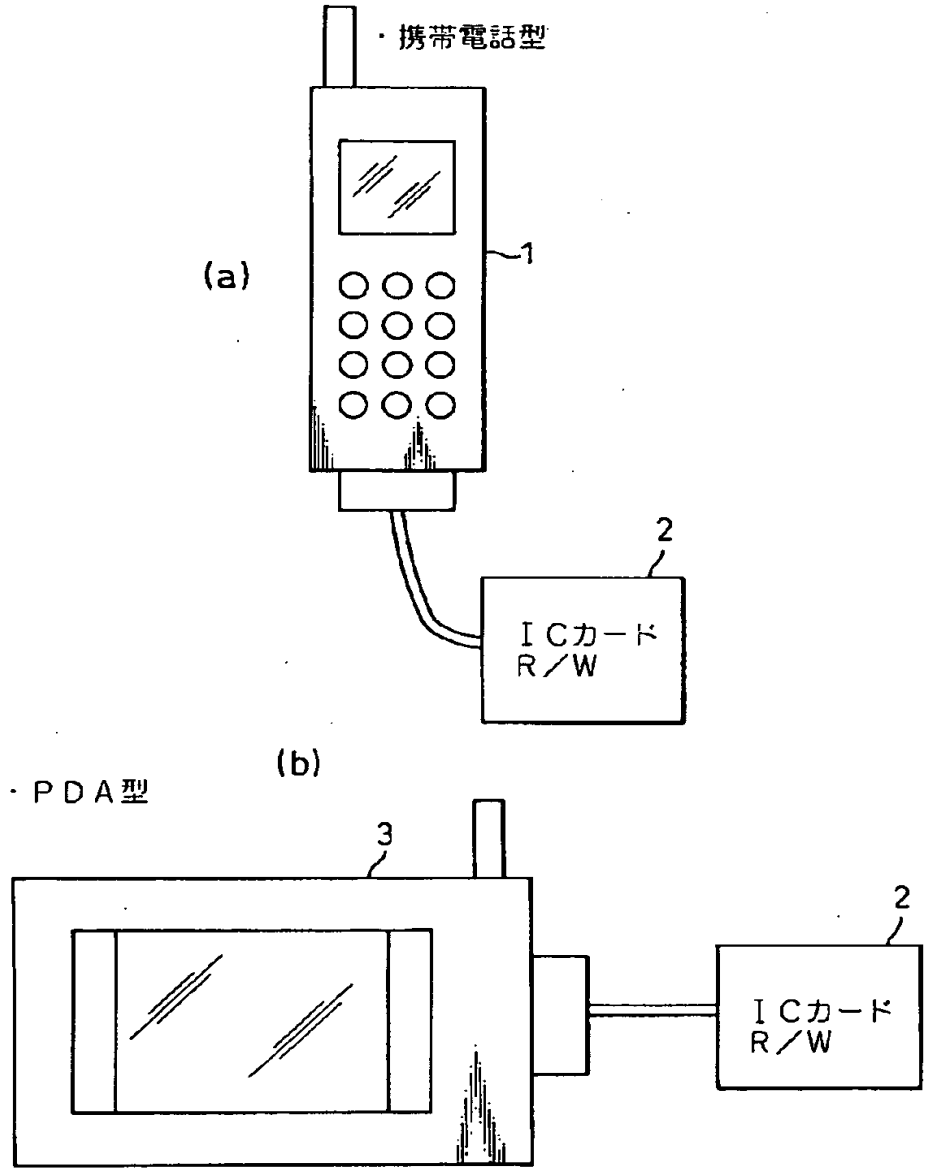
６０…決済端末

７０…無線通信モジュール

【書類名】　　図面

【図１】

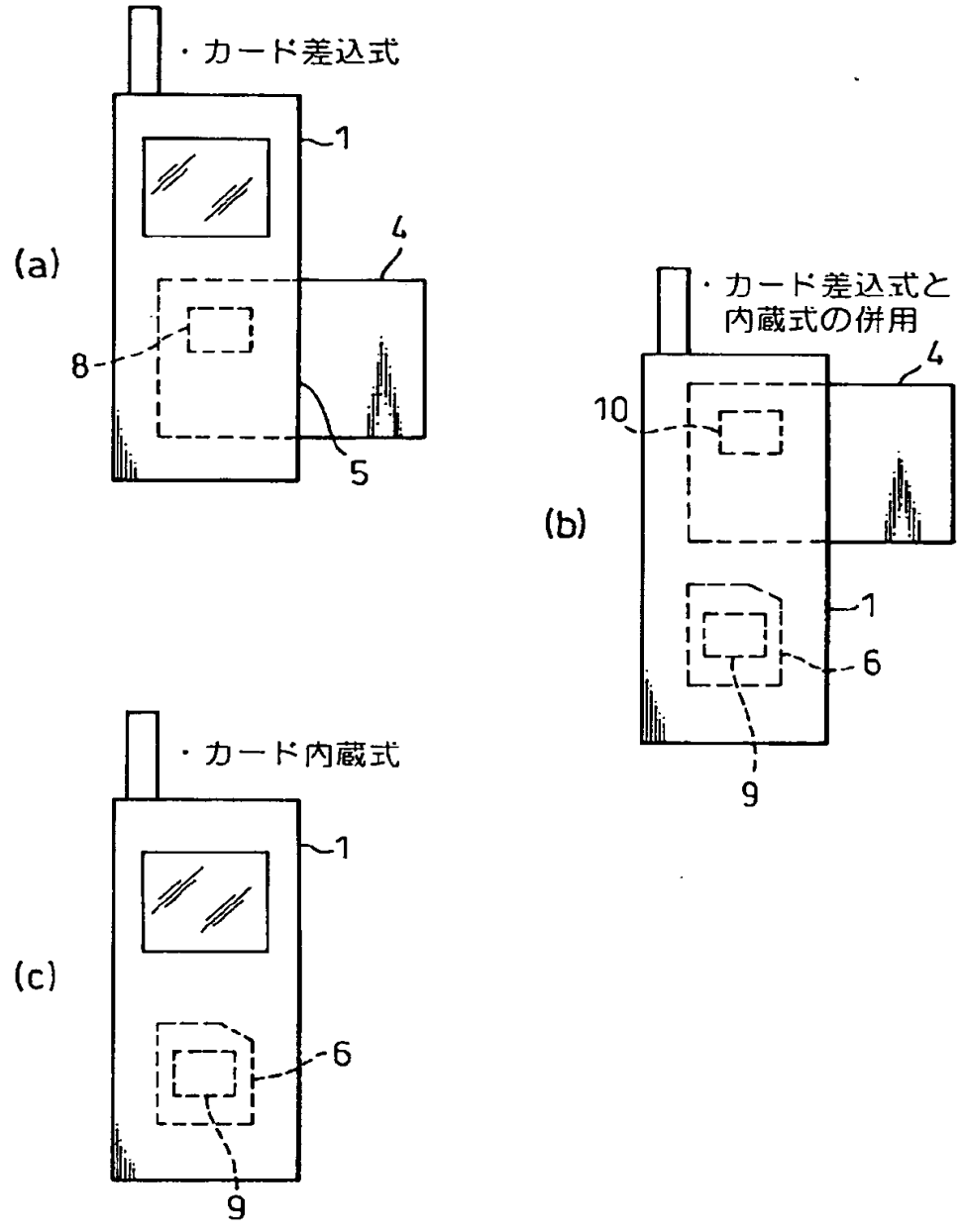
図1　　携帯情報端末



【図２】

図２

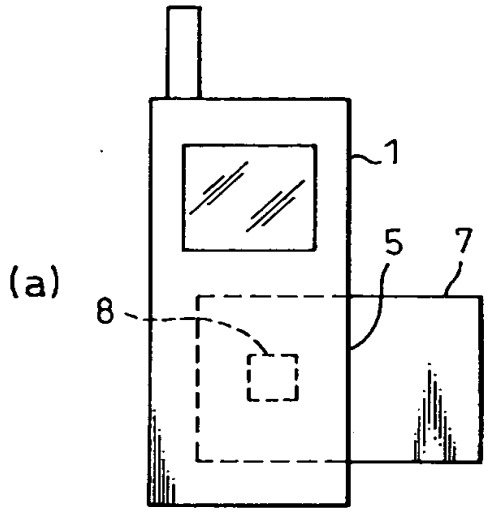
接触型ＩＣカードＲ／Ｗを内蔵



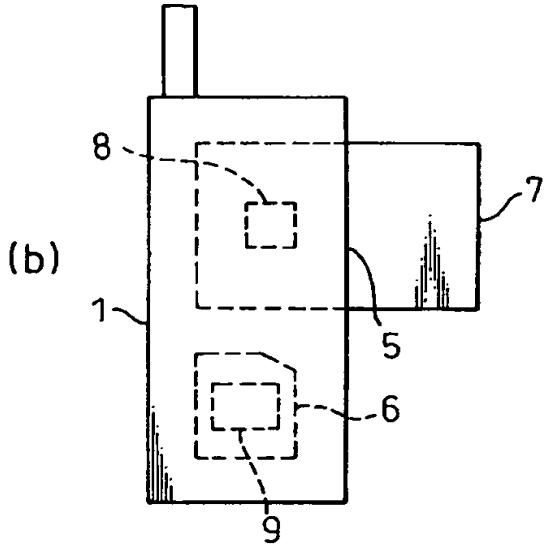
【図３】

図３

非接触型ＩＣカードＲ／Ｗを内蔵

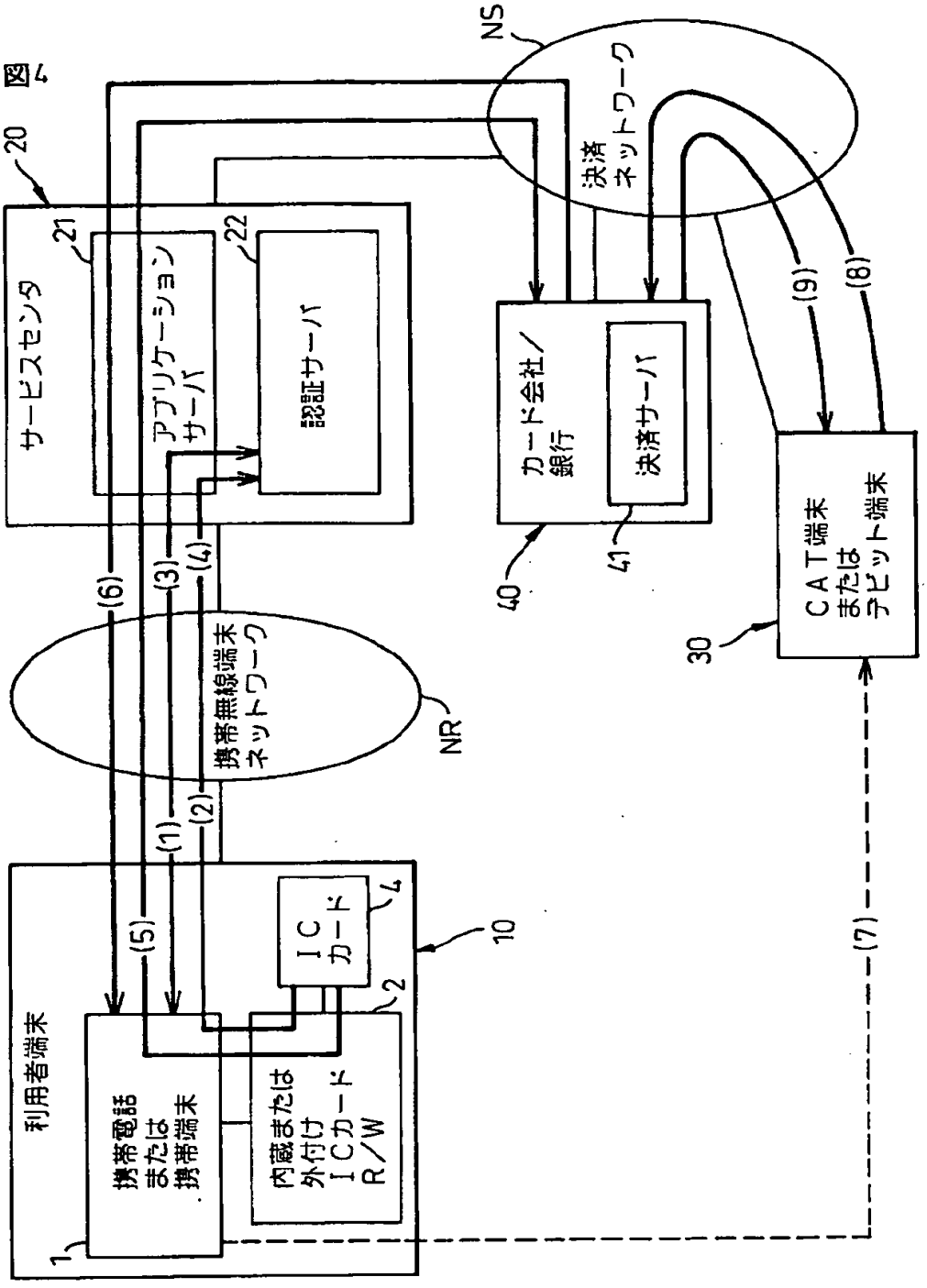


接触型ＩＣカードＲ／Ｗと
非接触型ＩＣカードＲ／Ｗの両方を内蔵



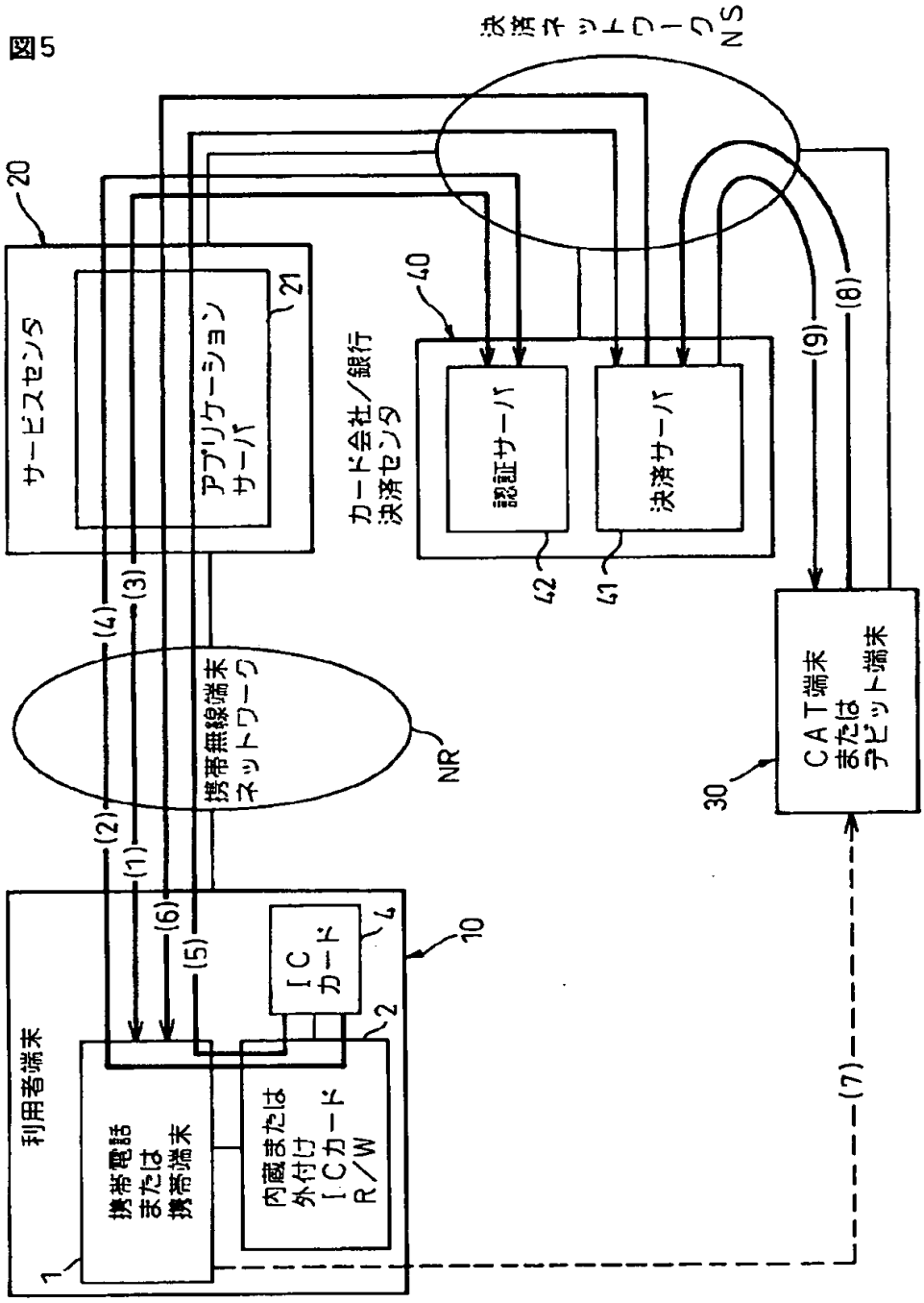
【図４】

図4


NS
決済ネットワーク
20
サービスセンタ
21
アプリケーションサーバ
22
認証サーバ
カード会社／銀行
決済サーバ
40
41
CAT端末またはデビット端末
30
(9)
(8)
(6)
(3)
(4)
携帯無線端末ネットワーク
NR
(1)
(2)
(5)
(7)
利用者端末
ICカード
4
10
2
携帯電話または携帯端末
内蔵または外付けICカードR／W
1

【図５】

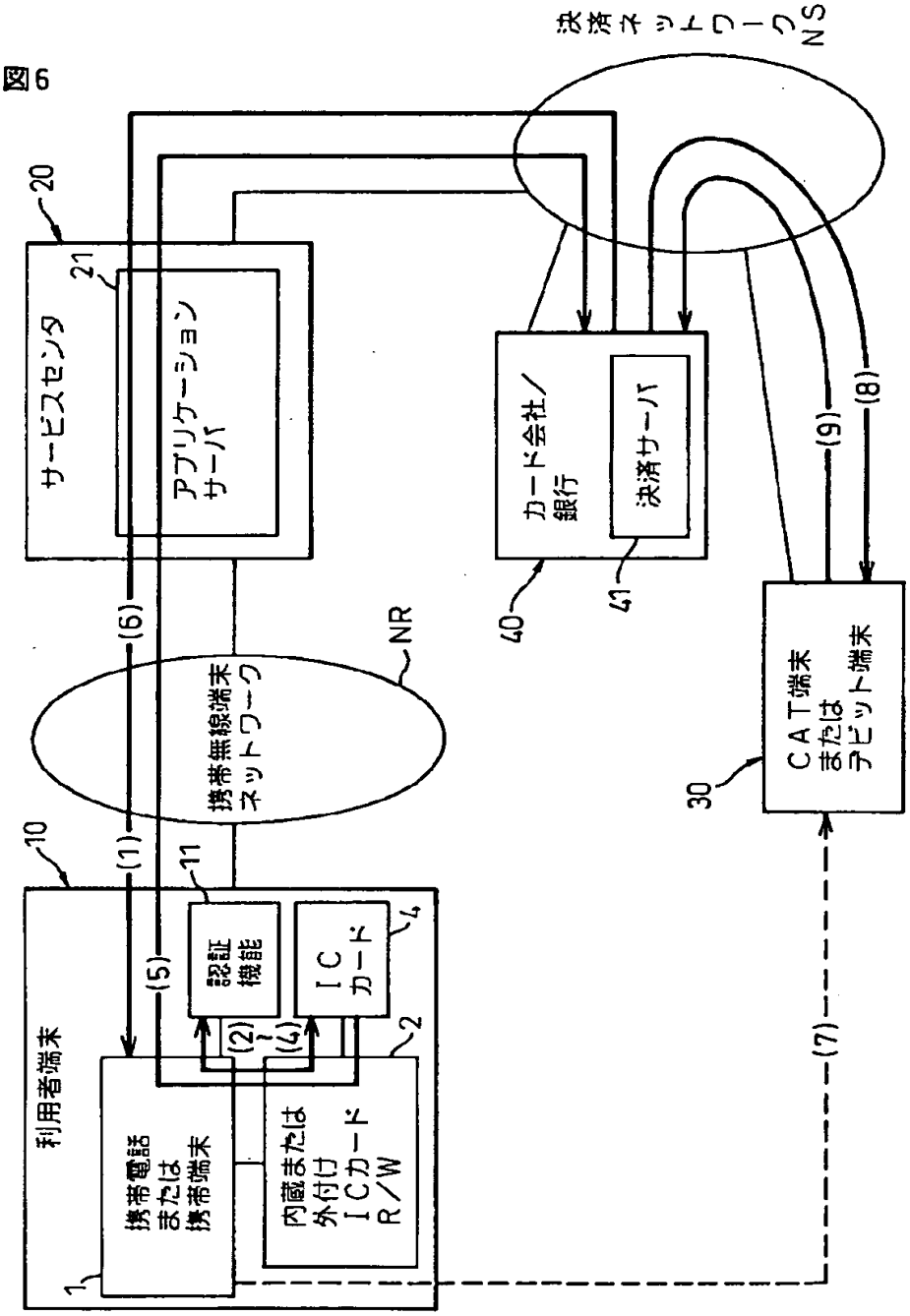
図5


決済ネットワーク NS
20
サービスセンタ
アプリケーション サーバ
21
40
カード会社／銀行 決済センタ
認証サーバ
決済サーバ
42
41
(8)
(9)
(4)
(3)
携帯無線端末 ネットワーク
NR
CAT端末 または デビット端末
30
(2)
(1)
(6)
(5)
IC カード
4
10
2
利用者端末
携帯電話 または 携帯端末
内蔵または 外付け ICカード R／W
1
(7)

【図６】

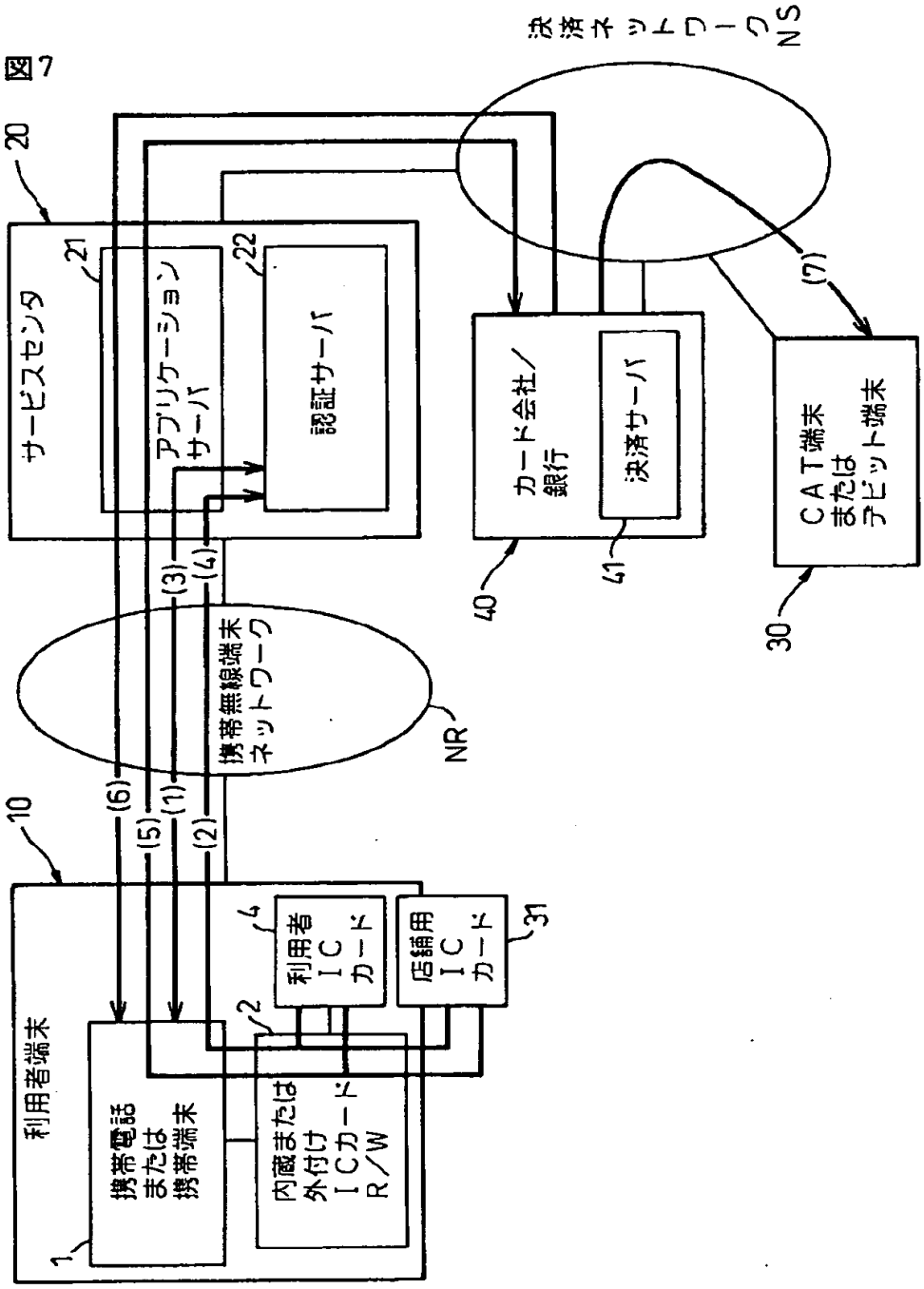
携帯端末の内部に認証機能を持つ場合

図6



【図７】

図7


決済ネットワーク NS
20
サービスセンタ
21
アプリケーション サーバ
22
認証サーバ
カード会社／ 銀行
決済サーバ
40
41
CAT端末 または デビット端末
30
(7)
(3)
(4)
携帯無線端末 ネットワーク
NR
(6)
(5)
(1)
(2)
10
利用者端末
4
利用者 IC カード
店舗用 IC カード
31
2
携帯電話 または 携帯端末
内蔵または 外付け IC カード R／W
1

【図８】

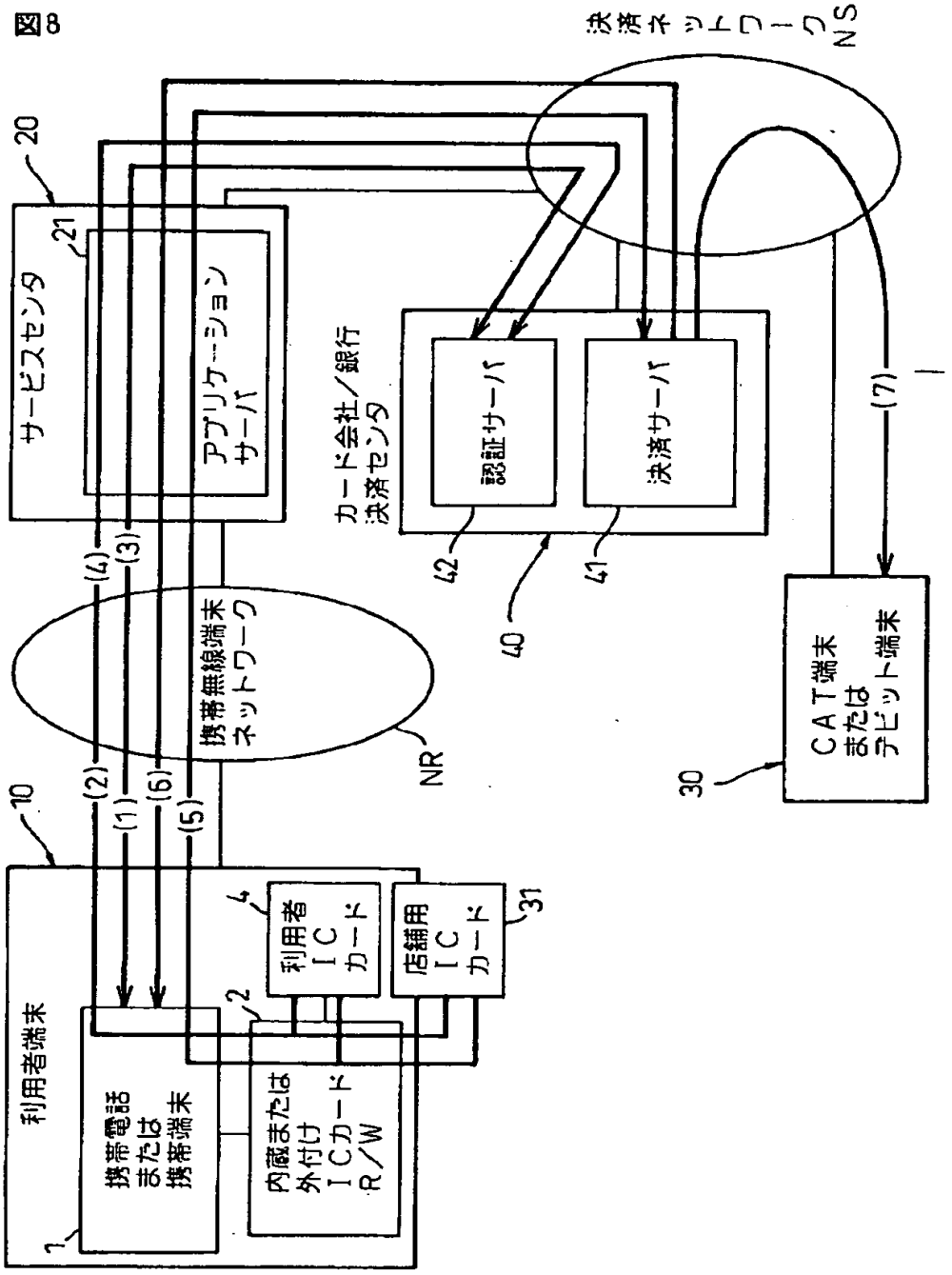
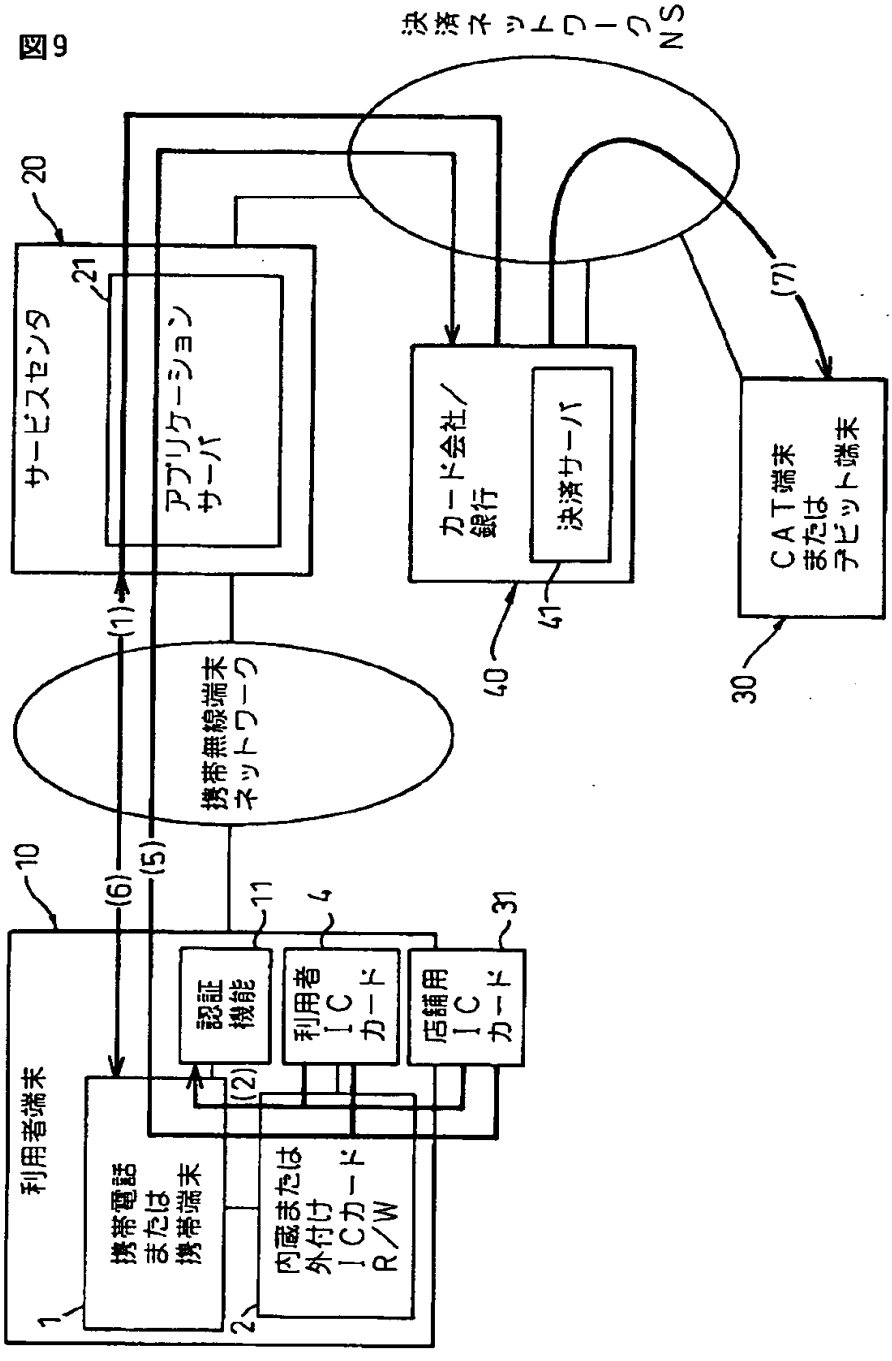


図8
決済ネットワーク NS
20
サービスセンタ
21
アプリケーション サーバ
カード会社／銀行 決済センタ
認証サーバ
決済サーバ
42
41
40
(7)
CAT端末 またはデビット端末
30
携帯無線端末 ネットワーク
NR
(2)
(1)
(6)
(5)
(4)
(3)
10
利用者端末
4
利用者 IC カード
店舗用 IC カード
31
2
携帯電話 または 携帯端末
内蔵または 外付け ICカード R／W
1

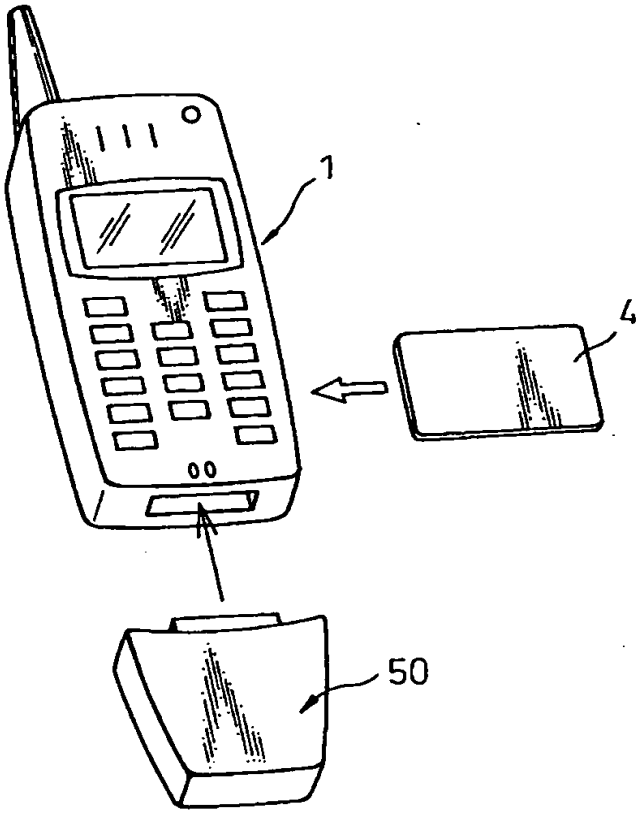
【図９】

図9


決済ネットワーク NS
20
サービスセンタ
21
アプリケーション サーバ
カード会社／ 銀行
決済サーバ
CAT端末 または デビット端末
(7)
40
41
30
(1)
携帯無線端末 ネットワーク
(6)
(5)
10
11
4
31
認証 機能
利用者 ICカード
店舗用 ICカード
(2)
利用者端末
携帯電話 または 携帯端末
内蔵または 外付け ICカード R／W
1
2

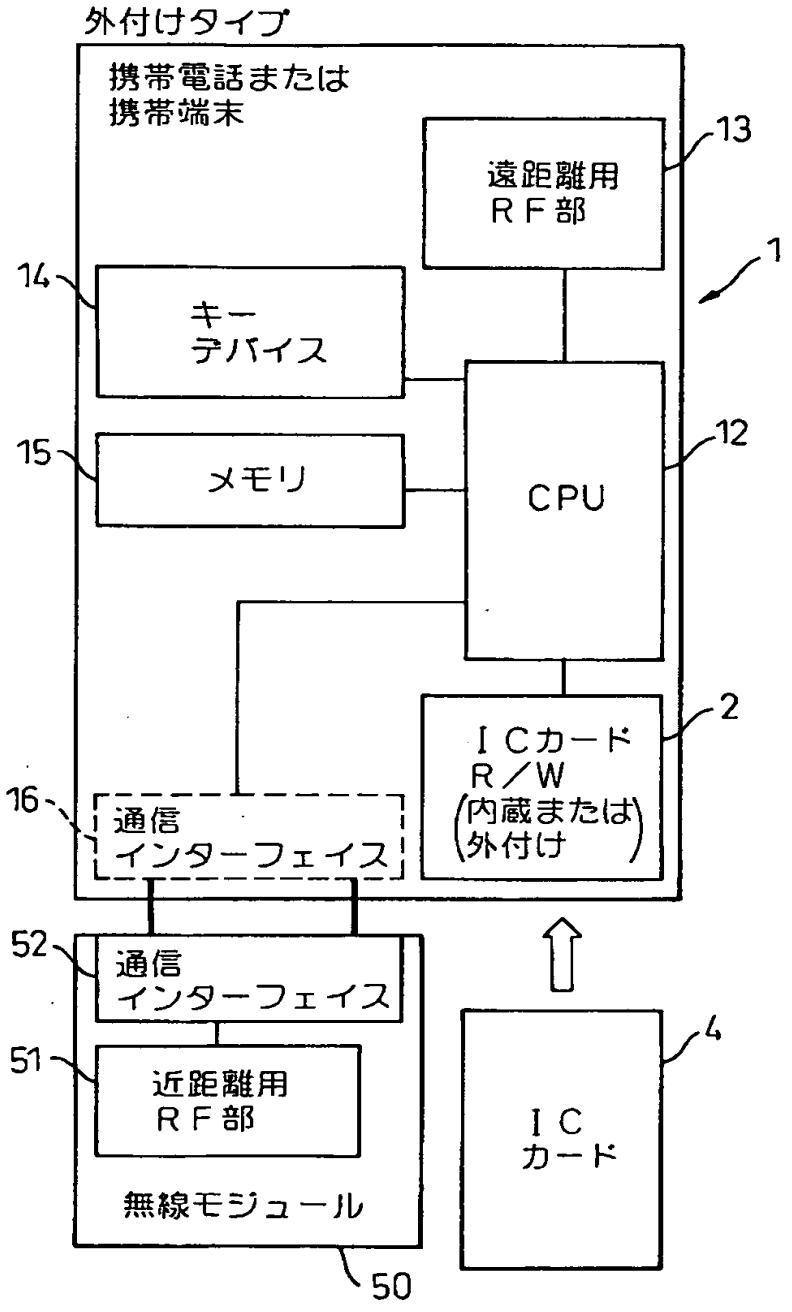
【図１０】

図10



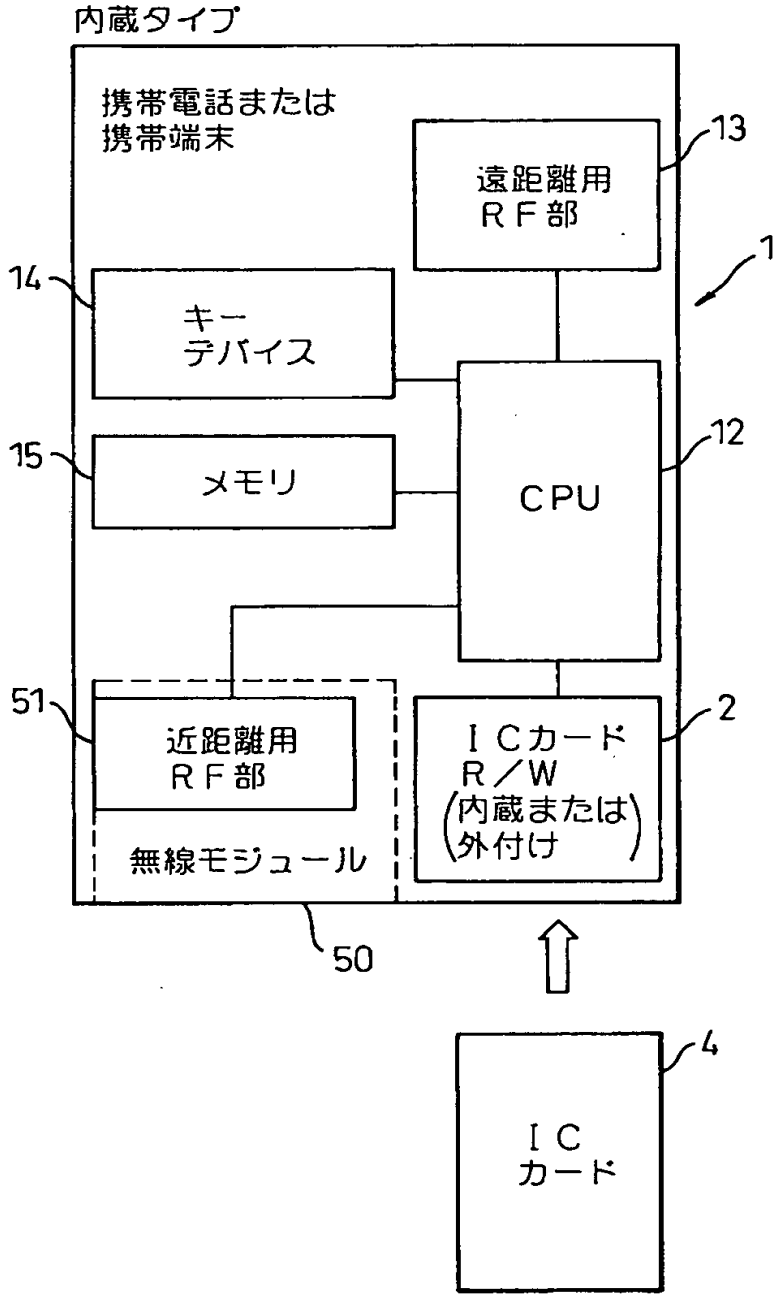
【図１１】

図11


外付けタイプ
携帯電話または
携帯端末
遠距離用
ＲＦ部
13
1
14
キー
デバイス
15
メモリ
CPU
12
ＩＣカード
Ｒ／Ｗ
(内蔵または
外付け)
2
16
通信
インターフェイス
52
通信
インターフェイス
51
近距離用
ＲＦ部
無線モジュール
50
ＩＣ
カード
4

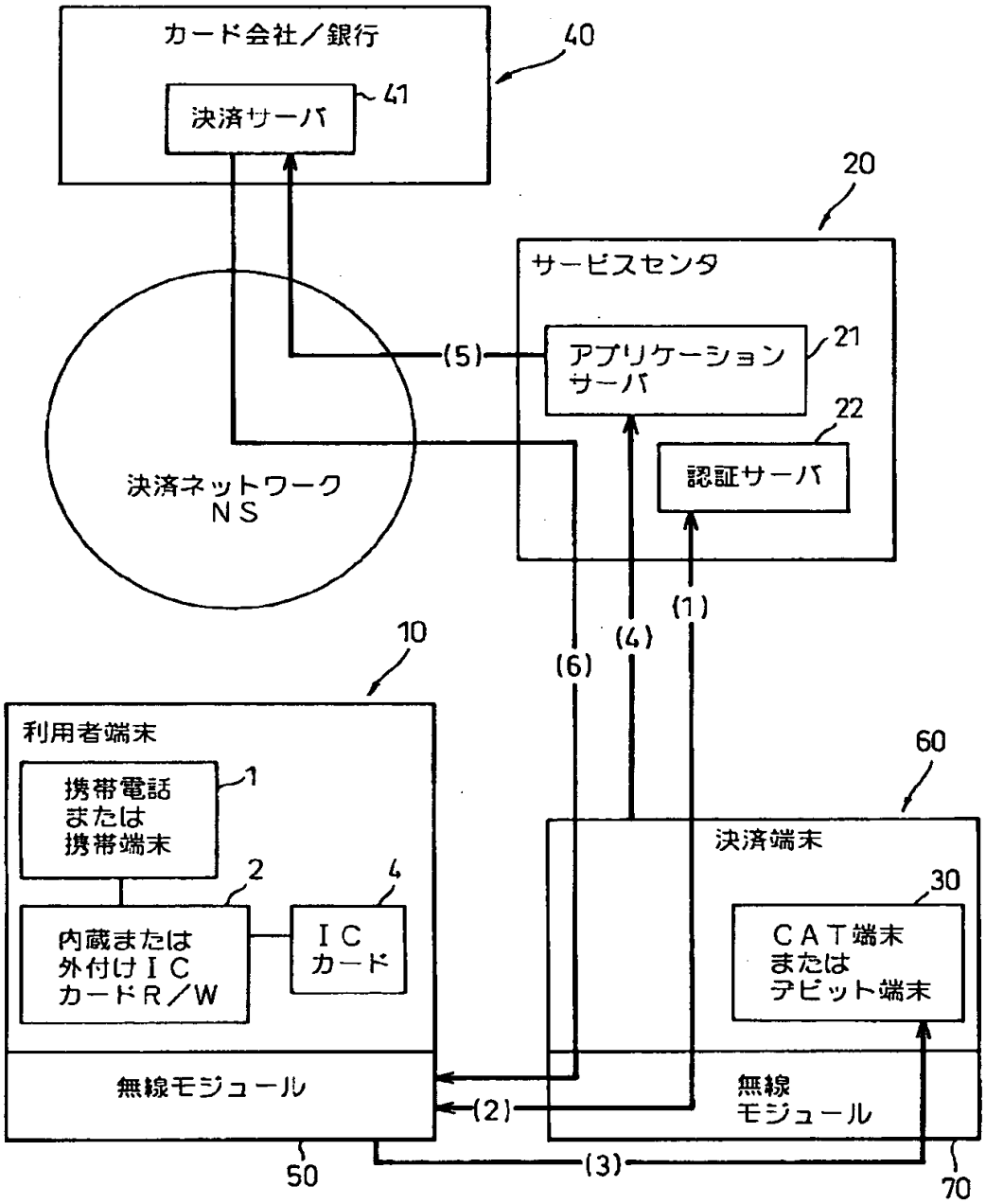
【図１２】

図12


内蔵タイプ
携帯電話または
携帯端末
遠距離用
ＲＦ部
13
1
14
キー
デバイス
15
メモリ
CPU
12
51
近距離用
ＲＦ部
無線モジュール
ＩＣカード
Ｒ／Ｗ
(内蔵または
外付け)
2
50
４
ＩＣ
カード

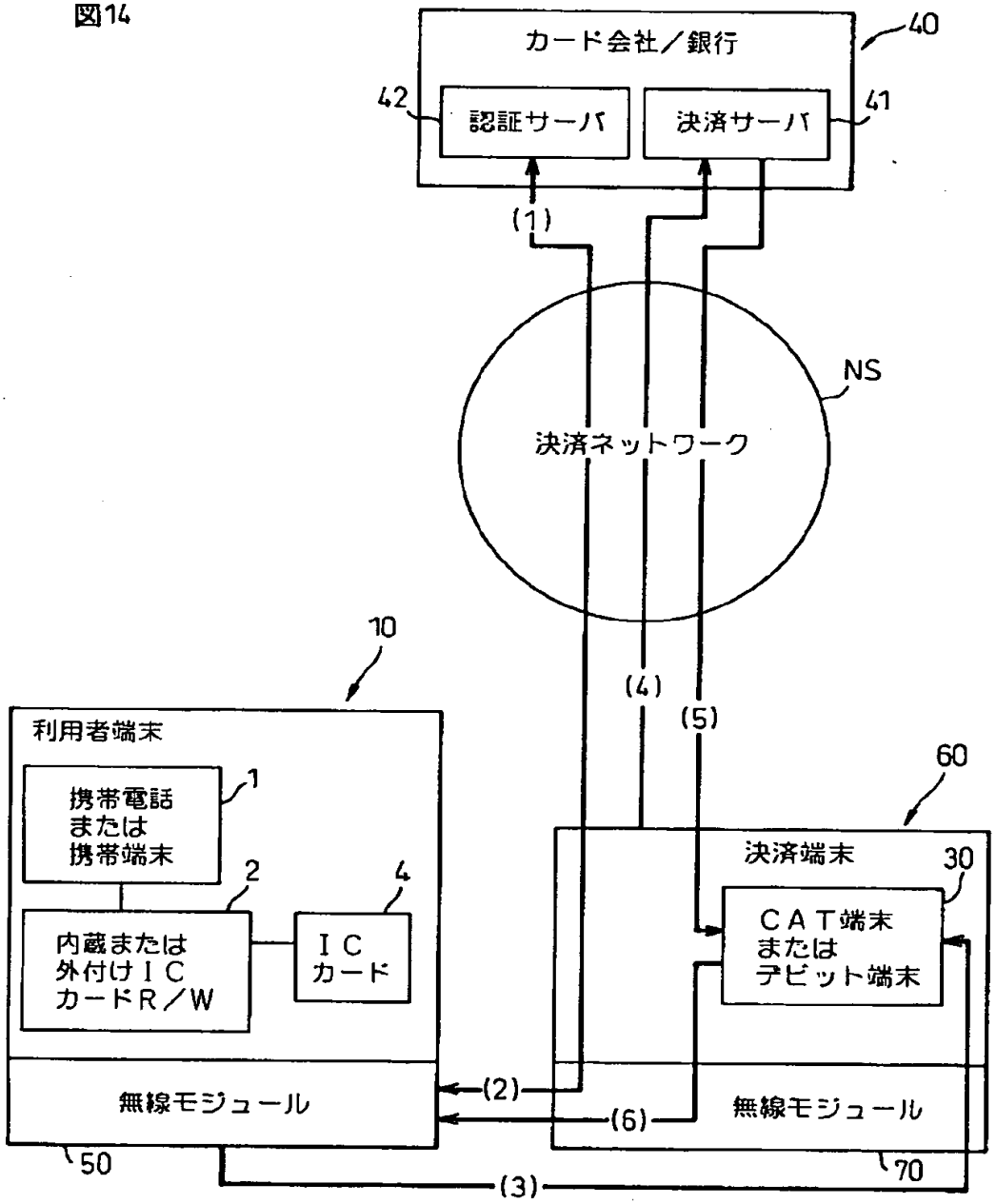
【図１３】

図13


カード会社／銀行
40
決済サーバ
41
20
サービスセンタ
(5)
アプリケーション
サーバ
21
22
認証サーバ
決済ネットワーク
ＮＳ
(1)
(4)
(6)
10
利用者端末
携帯電話
または
携帯端末
1
2
4
内蔵または
外付けＩＣ
カードＲ／Ｗ
ＩＣ
カード
60
決済端末
30
ＣＡＴ端末
または
デビット端末
無線モジュール
(2)
無線
モジュール
(3)
50
70

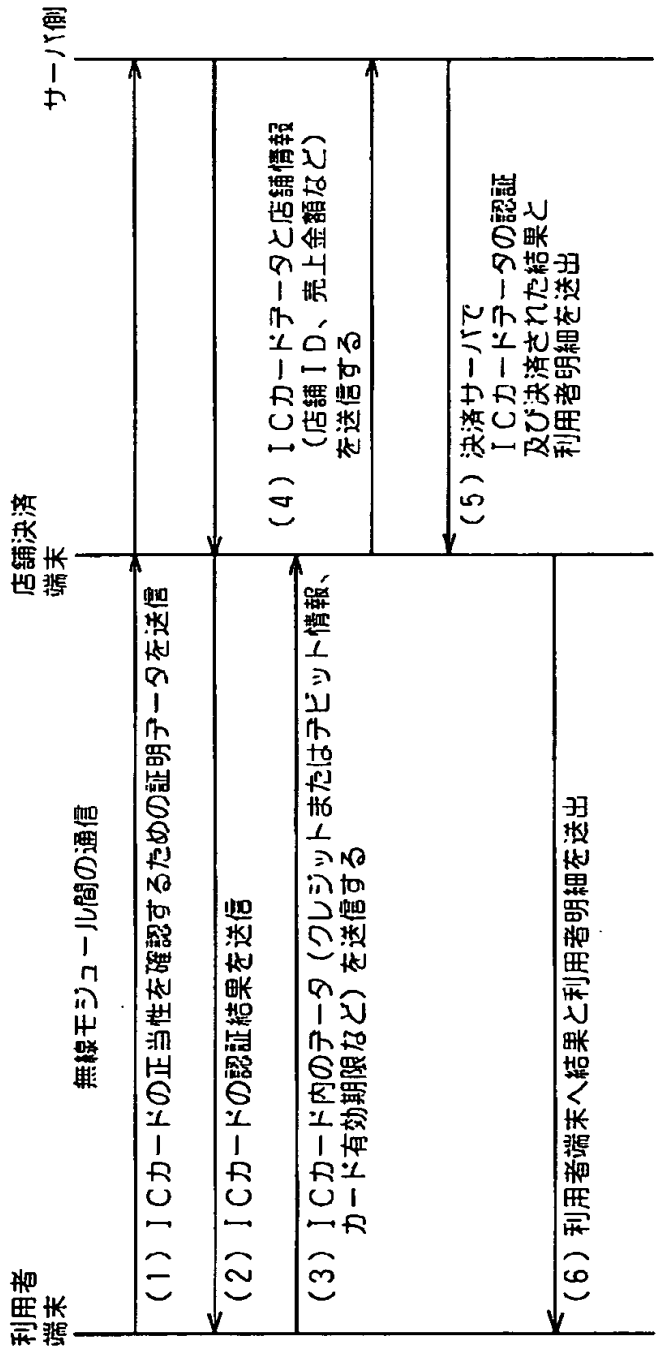
【図１４】

図14


カード会社／銀行
40
42
認証サーバ
決済サーバ
41
(1)
NS
決済ネットワーク
10
(4)
(5)
60
利用者端末
携帯電話
または
携帯端末
1
2
4
内蔵または
外付けＩＣ
カードＲ／Ｗ
ＩＣ
カード
決済端末
30
ＣＡＴ端末
または
デビット端末
無線モジュール
(2)
(6)
無線モジュール
50
70
(3)

【図１５】

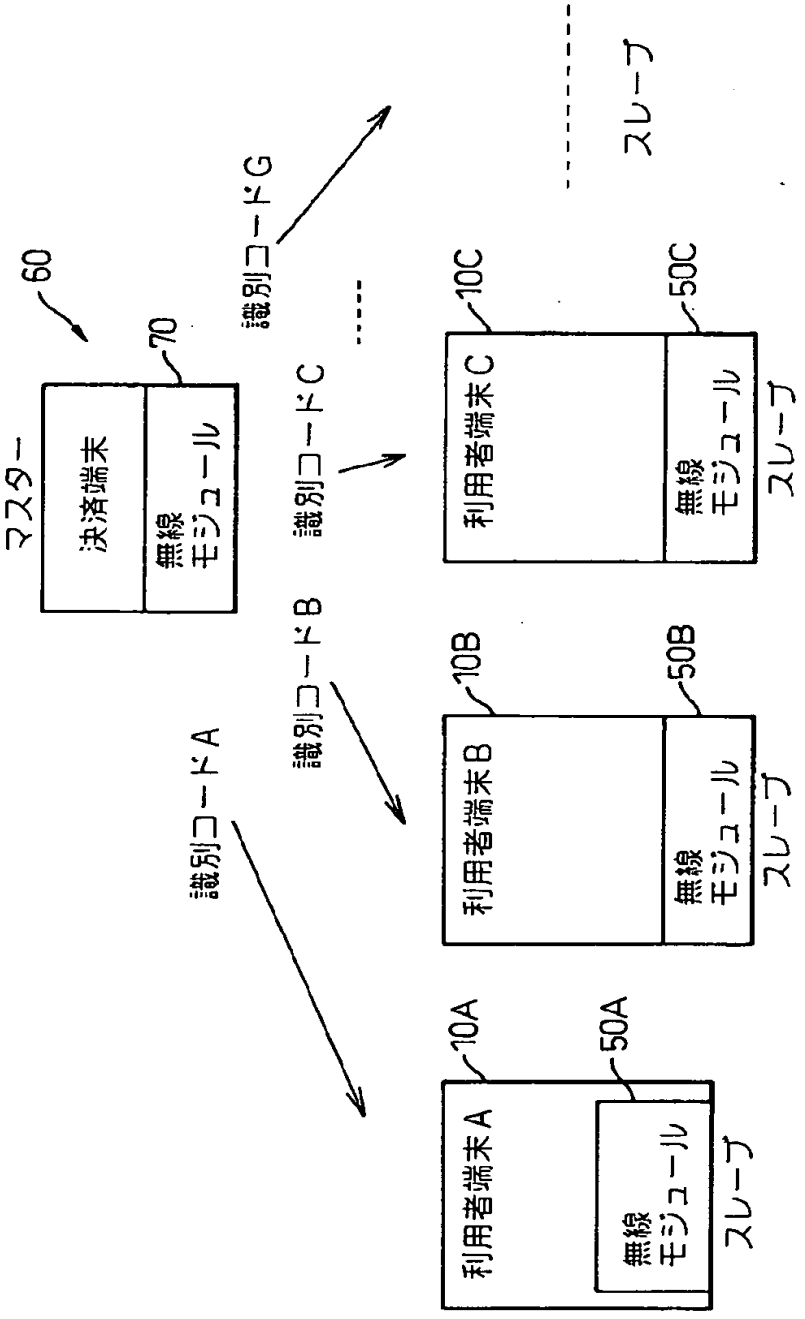
図15



＊無線モジュール間のデータは、利用する無線プロトコルの暗号方式を利用して暗号化する

【図１６】

図16


マスター
60
決済端末
70
無線モジュール
識別コードA
識別コードB
識別コードC
識別コードG
利用者端末A
10A
50A
無線モジュール
スレーブ
利用者端末B
10B
50B
無線モジュール
スレーブ
利用者端末C
10C
50C
無線モジュール
スレーブ
スレーブ

【書類名】　　要約書

【要約】

【課題】　ＩＣカード読み書き機能の付いた携帯情報端末を利用して、決済機能付のＩＣカードによる決済サービスを実現させて利便性を図る。

【解決手段】　既存のカード決済システムに加えて、ＩＣカードの読み書き可能な携帯情報端末１と、携帯情報端末のネットワークＮＲと決済ネットワークＮＳ間のゲートウエイ機能を提供するアプリケーションサーバ２１を設け、店舗において顧客がＩＣカード４を装着した携帯情報端末１からアプリケーションサーバ２１経由で認証サーバ２２に接続して認証情報とクレジット情報を認証サーバ２２に送出し、認証サーバ２２がＩＣカード４の適否を認証した後、クレジット情報に基づいて作成したワンタイムパスワードを携帯情報端末１の表示器に表示させ、店舗側がこのワンタイムパスワードと売上情報を決済端末３０から入力して決済が完了するシステムである。

【選択図】　　図４

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社